Corrections and Reentry: Protected Health Information Privacy Framework for Information Sharing Trust Interoperability Profile

Table of Contents

1. Overall Organization
2. Trustmark Definition Checklist
3. Corrections and Reentry: Protected Health Information Privacy Framework for Information Sharing Trust Interoperability Profile
   A. References
      α. Trustmark Definition Requirements
      β. Trust Interoperability Profiles
4. PHI Privacy Policy Trust Interoperability Profile
   A. References
      α. Trustmark Definition Requirements
      β. Trust Interoperability Profiles
5. Policy: Purpose Statement Trustmark Definition
   A. Metadata
   B. Conformance Criteria
      α. Policy: Purpose Statement
6. Policy: Policy Applicability and Legal Compliance Trustmark Definition
   A. Metadata
   B. Conformance Criteria
      α. Policy: Policy Applicability and Legal Compliance
7. Policy: Definitions Trustmark Definition
   A. Metadata
   B. Conformance Criteria
      α. Policy: Definitions
8. Information Sharing Policy: Acquiring and Receiving Information Trustmark Definition
   A. Metadata
   B. Conformance Criteria
      α. Information Sharing Policy: Acquiring and Receiving Information
9. PHI Privacy Policy: Program Evaluation and Research Trustmark Definition
   A. Metadata
   B. Conformance Criteria
      α. PHI Privacy Policy: Program Evaluation and Research

10. Information Sharing Policy: Merging Records Trustmark Definition
    A. Metadata
    B. Conformance Criteria
        α. Information Sharing Policy: Merging Records
11. PHI Privacy Policy: Use and Disclosure Trustmark Definition
    A. Metadata
    B. Conformance Criteria
        α. PHI Privacy Policy: Use and Disclosure
12. Redress Policy Trustmark Definition
    A. Metadata
    B. Conformance Criteria
        α. Redress Policy
13. Information Sharing Policy: Information Security Safeguards Trustmark Definition
    A. Metadata
    B. Conformance Criteria
        α. Information Sharing Policy: Information Security Safeguards
14. Information Sharing Policy: Information Retention and Destruction Trustmark Definition
    A. Metadata
    B. Conformance Criteria
        α. Information Sharing Policy: Information Retention and Destruction
15. Information Sharing Policy: Training Trustmark Definition
    A. Metadata
    B. Conformance Criteria
        α. Information Sharing Policy: Training
16. PHI Privacy Policy: Governance and Oversight Trust Interoperability Profile
    A. References
        α. Trustmark Definition Requirements
        β. Trust Interoperability Profiles
17. PHI Privacy Policy: Governance and Oversight Trustmark Definition
    A. Metadata
    B. Conformance Criteria
        α. PHI Privacy Policy: Governance and Oversight
18. Information Sharing Policy: Governance and Oversight Trustmark Definition
    A. Metadata
    B. Conformance Criteria
        α. Information Sharing Policy: Governance and Oversight
19. PHI Privacy Policy: Information Trust Interoperability Profile
    A. References
        α. Trustmark Definition Requirements
        β. Trust Interoperability Profiles
20. PHI Privacy Policy: Information Trustmark Definition
    A. Metadata
    B. Conformance Criteria
        α. PHI Privacy Policy: Information
21. Information Sharing Policy: Information Trustmark Definition
    A. Metadata
    B. Conformance Criteria
        α. Information Sharing Policy: Information

22. PHI Privacy Policy: Information Quality Assurance Trust Interoperability Profile
A. References
α. Trustmark Definition Requirements
β. Trust Interoperability Profiles
23. PHI Privacy Policy: Information Quality Assurance Trustmark Definition
A. Metadata
B. Conformance Criteria
α. PHI Privacy Policy: Information Quality Assurance
24. Information Sharing Policy: Information Quality Assurance Trustmark Definition
A. Metadata
B. Conformance Criteria
α. Information Sharing Policy: Information Quality Assurance
25. PHI Privacy Policy: Accountability and Enforcement Trust Interoperability Profile
A. References
α. Trustmark Definition Requirements
β. Trust Interoperability Profiles
26. PHI Privacy Policy: Accountability and Enforcement Trustmark Definition
A. Metadata
B. Conformance Criteria
α. PHI Privacy Policy: Accountability and Enforcement
27. Information Sharing Policy: Accountability and Enforcement Trustmark Definition
A. Metadata
B. Conformance Criteria
α. Information Sharing Policy: Accountability and Enforcement
28. Consent Authorizations Profile Trust Interoperability Profile
A. References
α. Trustmark Definition Requirements
β. Trust Interoperability Profiles
29. Consent Authorization Revocation Trustmark Definition
A. Metadata
B. Conformance Criteria
α. Authorization Revocation
30. Consent Authorization Form Requirements Profile Trust Interoperability Profile
A. References
α. Trustmark Definition Requirements
β. Trust Interoperability Profiles
31. HIPAA Consent Authorization Form Requirements Trustmark Definition
A. Metadata
B. Conformance Criteria
α. HIPAA Consent Authorization Form Requirements - Elements
β. HIPAA Consent Authorization Form Requirements - Notice Statements
32. 42 CFR Part 2 Consent Authorization Form Requirements Trustmark Definition
A. Metadata
B. Conformance Criteria
α. 42 CFR Part 2 Consent Authorization Form Requirements - Elements
β. 42 CFR Part 2 Consent Authorization Form Requirements - Notice Statements
33. Defective Consent Authorizations Profile Trust Interoperability Profile
A. References

    α. Trustmark Definition Requirements
    β. Trust Interoperability Profiles
34. HIPAA Defective Consent Authorizations Trustmark Definition
  A. Metadata
  B. Conformance Criteria
    α. HIPPA Defective Authorizations
    β. Compound Authorizations
    γ. Prohibition on Conditioning of Authorizations
35. 42 CFR Part 2 Defective Consent Authorizations Trustmark Definition
  A. Metadata
  B. Conformance Criteria
    α. HIPAA Consent Authorization Form Requirements - Elements
36. Contractual Agreements Profile Trust Interoperability Profile
  A. References
    α. Trustmark Definition Requirements
    β. Trust Interoperability Profiles
37. HIPAA Business Associate Trustmark Definition
  A. Metadata
  B. Conformance Criteria
    α. Valid HIPAA Business Associate
38. Business Associate/Qualified Service Organization Agreements Trustmark Definition
  A. Metadata
  B. Conformance Criteria
    α. Contractual Agreements with HIPPA-Covered Entities
39. Redress Policy Trustmark Definition
  A. Metadata
  B. Conformance Criteria
    α. Redress Policy
40. Glossary

Overall Organization

- Corrections and Reentry: Protected Health Information Privacy Framework for Information Sharing TIP
  - PHI Privacy Policy TIP
    - Policy: Purpose Statement TD
    - Policy: Policy Applicability and Legal Compliance TD
    - Policy: Definitions TD
    - Information Sharing Policy: Acquiring and Receiving Information TD
    - PHI Privacy Policy: Program Evaluation and Research TD
    - Information Sharing Policy: Merging Records TD
    - PHI Privacy Policy: Use and Disclosure TD
    - Redress Policy TD
    - Information Sharing Policy: Information Security Safeguards TD
    - Information Sharing Policy: Information Retention and Destruction TD
    - Information Sharing Policy: Training TD
    - PHI Privacy Policy: Governance and Oversight TIP
      - PHI Privacy Policy: Governance and Oversight TD
      - Information Sharing Policy: Governance and Oversight TD
    - PHI Privacy Policy: Information TIP
      - PHI Privacy Policy: Information TD
      - Information Sharing Policy: Information TD
    - PHI Privacy Policy: Information Quality Assurance TIP
      - PHI Privacy Policy: Information Quality Assurance TD
      - Information Sharing Policy: Information Quality Assurance TD
    - PHI Privacy Policy: Accountability and Enforcement TIP
      - PHI Privacy Policy: Accountability and Enforcement TD
      - Information Sharing Policy: Accountability and Enforcement TD
  - Consent Authorizations Profile TIP
    - Consent Authorization Revocation TD
    - Consent Authorization Form Requirements Profile TIP
      - HIPAA Consent Authorization Form Requirements TD
      - 42 CFR Part 2 Consent Authorization Form Requirements TD
    - Defective Consent Authorizations Profile TIP
      - HIPAA Defective Consent Authorizations TD
      - 42 CFR Part 2 Defective Consent Authorizations TD
  - Contractual Agreements Profile TIP
    - HIPAA Business Associate TD

- Business Associate/Qualified Service Organization Agreements TD
- Redress Policy TD

Trustmark Definition Checklist

Policy: Purpose Statement

- [ ] **Policy Purpose**: Does the entity's policy clearly state the purpose of establishing a privacy, civil rights, and civil liberties protection policy (i.e., what does the entity hope to accomplish in adopting this policy)? [assessment_01]

Issuance Criteria:
yes(ALL)

Policy: Policy Applicability and Legal Compliance

- [ ] **Subject to Policy**: Does the entity's policy clearly state who is subject to the policy (who must comply with the policy; for example, entity personnel, participating agencies, and private contractors)? [assessment_01]
- [ ] **Policy Dissemination**: Does the entity's policy clearly state the method(s) by which the policy is made available to personnel, participating entities, and individual users (for example, in print, online, etc.) and whether the entity requires personnel, participating entities, and individual users to acknowledge receipt of the policy and agreement to comply with the policy in writing? [assessment_02]
- [ ] **Requirement of Law Compliance**: Does the entity's policy clearly state that personnel and participating information-originating and user agencies must be in compliance with all applicable law protecting privacy, civil rights, and civil liberties in the gathering and collection, use, analysis, retention, destruction, sharing, disclosure, and dissemination of medical, mental health, and substance abuse information and list the primary laws with which personnel and participating users must comply? [assessment_03]
- [ ] **Internal Policies in Compliance with Laws**: Does the entity's policy clearly state whether the entity's internal operating policies are in compliance with all applicable law protecting privacy, civil rights, and civil liberties in the gathering and collection, use, analysis, retention, destruction, sharing, disclosure, and dissemination of medical, mental health, and substance abuse information, and are the laws with which internal operation policies must be in compliance cited in the privacy policy? [assessment_04]

Issuance Criteria:
yes(ALL)

Policy: Definitions

- [ ] **Term Definitions**: Does the entity's policy clearly state the key words or phrases (and definitions) that are regularly used in the policy for which the entity wants to specify particular meanings? [assessment_01]

Issuance Criteria:
yes(ALL)

Information Sharing Policy: Acquiring and Receiving Information

- [ ] **Sharing Agencies Adhere to Laws and Policies**: Does the entity's information sharing policy clearly state whether the agencies that access your entity's PHI and/or share PHI with your entity ensure that they will adhere to applicable laws and policies? [move to PHI?] [assessment_01]
- [ ] **Compliance Assurance for Commercial Database Providers**: Does the entity's information sharing policy clearly state whether the entity contracts with commercial databases and, if so, how the entity ensures that the commercial database company is in legal compliance in its information-gathering techniques? [assessment_02]

Issuance Criteria:
yes(ALL)

PHI Privacy Policy: Program Evaluation and Research

- [ ] **Authorization to Analyze Deidentified PHI**: Does the entity's PHI privacy policy clearly state who is authorized (position/title, credentials, etc.) to analyze deidentified PHI for evaluation and research purposes? [assessment_01]
- [ ] **Determination of Which Deidentified PHI to Analyze**: Does the entity's PHI privacy policy clearly state what deidentified PHI is analyzed? [assessment_02]
- [ ] **Purpose for Analyzing Deidentified PHI**: Does the entity's PHI privacy policy clearly state for what purpose(s) is the deidentified PHI analyzed? [assessment_03]

Issuance Criteria:
yes(ALL)

Information Sharing Policy: Merging Records

- [ ] **Persons Authorized to Merge Records**: Does the entity's information sharing policy clearly state who is authorized (position/title, credentials, etc.) to merge records? [assessment_01]
- [ ] **Criteria for Merging**: Does the entity's information sharing policy clearly state what matching criteria the entity requires when attempting to merge information from multiple records allegedly about the same individual? In other words, when two records are compared for possible merger, are there certain attributes (name, date of birth, social security number, etc.) that must match, or is

there a minimum number of attributes (for example, two out of five) that must match to link the two records as relating to the same person? [assessment_02]

- [ ] **Associating Records not Meeting Merge Criteria**: Does the entity's information sharing policy clearly state the entity's procedure for associating records, if the criteria specified in 2 above are not met? (Note: If the entity does not merge or associate records that have partial matches, then the policy should so state.) [assessment_03]

Issuance Criteria:
yes(ALL)

PHI Privacy Policy: Use and Disclosure

- [ ] **Controlled Actions and Permissions of PHI Recipients**: Does the entity's PHI privacy policy clearly state what types of information recipient actions and permissions are controlled by the entity's access or dissemination limitations? Best practice: It is suggested that entities specify their method for identifying information recipient actions and permissions in their privacy policies. (Note: Information recipient actions and permissions are often used to identify entities and individuals with a need and right to know particular information; to access case management information (including medical, mental health, and/or substance abuse information); access nonpersonally identifiable information only; or to identify who is authorized to submit or modify particular records or record sets, to have read-only access or to be authorized to add/modify/delete records, or to be authorized to grant privileges.) [assessment_01]
- [ ] **Implemented Limits on Disclosure**: Does the entity's PHI privacy policy clearly state what limitations the entity has implemented to limit or restrict disclosure of PHI? [assessment_02]
- [ ] **Conditions and Credentials for Access and Disclosure and Audit Trails Thereof**: Does the entity's PHI privacy policy clearly state the conditions and credentials by which access to and disclosure of PHI records retained by the entity will be provided within the entity or in other governmental agencies, and whether an audit trail is kept of access to and disclosure of PHI retained by the entity (e.g., dissemination logs, algorithms)? [assessment_03]
- [ ] **Conditions Requiring Individual Consent Authorization**: Does the entity's PHI privacy policy clearly state the conditions by which access to and disclosure of PHI retained by the entity are not permitted without an individual consent authorization? [assessment_04]
- [ ] **Released Individual Restriction and Nondisclosure Requests**: Does the entity's PHI privacy policy clearly state whether the entity permits released individuals (those who are no longer in lawful custody) to request that the entity restrict the use and disclosure of the individuals' PHI retained by the entity? [assessment_05]
- [ ] **Disclosure for Released Individuals**: Does the entity's PHI privacy policy clearly state, for individuals who are released from custody (for example, on probation or parole), the conditions by which the entity may use or disclose PHI without the individuals' written consent authorization? [assessment_06]
- [ ] **Originator Approval Required**: Does the entity's PHI privacy policy clearly state whether participating agencies that access information from the entity are required to obtain approval from

the originator of the information prior to further dissemination or to follow the disclosure or redisclosure law applicable to the originating agency, and, if the information is substance abuse information, does the entity provide the required 42 CFR Part 2 notice covering the disclosure of such information, along with any such disclosure of the substance abuse information? [assessment_07]

- [ ] **Conditions for Medical/Mental Health/Behavioral Health Release and Audit Trails Thereof**: Does the entity's PHI privacy policy clearly state the conditions under which access to and disclosure of PHI records retained by the entity will be provided to those responsible for medical, mental health and/or behavioral health, including substance use services, and whether an audit trail is kept of access to and disclosure of information retained by the entity (e.g., dissemination logs, algorithms)? [assessment_08]
- [ ] **Conditions for Public Release and Audit Trails Thereof**: Does the entity's PHI privacy policy clearly state under what circumstances and what legal authority will access to and disclosure of a record be provided to a member of the public in response to an information request, and whether these circumstances are described in the entity's redress policy, and whether an audit trail is kept of access to and disclosure of information retained by the entity without the audit trail constituting an impermissible collection of information of a member of the public (e.g., dissemination logs, algorithms)? (Note: This does not apply to circumstances in which an entity chooses to provide nonsensitive information to the public or to provide sensitive information in accordance with entity policy in response to an emergency situation.) [assessment_09]
- [ ] **Conditions for Specific Release and Audit Trails Thereof**: Does the entity's PHI privacy policy clearly state the conditions under which release of information retained by the entity can be made for specific purposes or to specific persons, and whether an audit trail is kept showing how those conditions were met? [assessment_10]
- [ ] **Disallowed Entities and Circumstances**: Does the entity's PHI privacy policy clearly state under what circumstances and to whom the entity will not disclose PHI records? [assessment_11]
- [ ] **Categories Not Ordinarily Public**: Does the entity's PHI privacy policy clearly state the categories of records that ordinarily will not be provided to the public pursuant to applicable legal authority, and citations to applicable legal authority for each stated category? [assessment_12]
- [ ] **Existence Confirmation to Ineligible Entities**: Does the entity's PHI privacy policy clearly state the entity's policy on confirming the existence or nonexistence of information to persons or agencies that are not eligible to receive the information? [assessment_13]

Issuance Criteria:
yes(ALL)

Redress Policy

- [ ] **Disclosure Notice**: Does the organization's Redress Policy disclose to individual about whom the information was gathered the conditions under which the entity will disclose PHI information? [assessment_01]
- [ ] **Disclosure Record**: Does the organization keep a record of all requests and of what information is

disclosed to an individual? [assessment_02]

- [ ] **Disclosure Exceptions**: Does the organization document exceptions when the individual about whom the information was gathered is not notified? This includes whether the entity refers the individual to the agency originating the information? [assessment_03]
- [ ] **Data Amendments**: Does the organization perform any of the following functions or activities that involve the use or disclosure of PHI on behalf of a covered entity? (Claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, or repricing.) [assessment_04]
- [ ] **Data Amendment Point of Contact**: Does the organization provide any of the following services that involve the use or disclosure of PHI to a covered entity? (Legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial.) [assessment_05]
- [ ] **Data Amendment Retention Record**: Does the organization provide any of the following services that involve the use or disclosure of PHI to a covered entity? (Legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial.) [assessment_06]
- [ ] **Data Amendment Point of Contact**: Does the organization provide a point of contact for handling individuals' requests for amendments of PHI? [assessment_07]
- [ ] **Data Amendment Procedure**: Does the organization have a procedure for handling individuals' requests for correction (or amendments) involving information that the entity can change because it originated the information? [assessment_08]
- [ ] **Data Amendment Record**: Does the organization maintain a record of requests for corrections (amendments) [assessment_09]
- [ ] **Appeal Conditions**: Does the organization document the conditions under which the entity may deny an individual's request for access or correction (amendment)? [assessment_10]
- [ ] **Appeal Procedure**: If requests for access or corrections (amendments) are denied, does the entity have a procedure for appeal (or review)? [assessment_11]

Issuance Criteria:
yes(ALL)

Information Sharing Policy: Information Security Safeguards

- [ ] **Designated Security Officer**: Does the entity's information sharing policy clearly state whether the entity has a designated information security officer, whether training is provided for the information security officer, and, if the role is a component of another position, whether the policy identifies the title of the position upholding security officer responsibilities? [assessment_01]
- [ ] **Safeguards for Data Security**: Does the entity's information sharing policy clearly state the entity's physical, procedural, and technical safeguards for ensuring the security of entity data? (Does the policy describe how the entity will protect the information from unauthorized access, modification, theft, sabotage, or destruction [whether internal or external] resulting from natural or human- caused disasters or intrusions with, for example, procedures, practices, system protocols,

use of software, information technology tools, process for data backups, and physical security measures?) [assessment_02]

- [ ] **Secure Format and Storage Environment**: Does the entity's information sharing policy clearly state the requirements that ensure that the information will be stored in a secure format and a secure environment? [assessment_03]
- [ ] **Assessment of Risks and Vulnerabilities of Held PHI**: Does the entity's information sharing policy clearly state if the entity is a HIPAA-covered entity, whether the entity has conducted an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the entity? [assessment_04]
- [ ] **Credentials for Authorized Access**: Does the entity's information sharing policy clearly state the required credentials of entity personnel authorized to have access to entity information? [assessment_05]
- [ ] **User-Identified Access**: Does the entity's information sharing policy clearly state whether electronic access to entity data identifies the user? [assessment_06]
- [ ] **Access Log and Audit Trail**: Does the entity's information sharing policy clearly state whether a log is kept of accessed and disseminated entity data, and whether an audit trail is maintained? [assessment_07]
- [ ] **Inactive Session Termination**: Does the entity's information sharing policy clearly state whether the entity has electronic procedures for terminating an electronic session after a period of inactivity? [assessment_08]
- [ ] **Risk and Vulnerability Assessments Separate from Public Data**: Does the entity's information sharing policy clearly state whether risk and vulnerability assessments (if maintained) are stored separately from publicly available data? [assessment_09]
- [ ] **Response to Security Incidents**: Does the entity's information sharing policy clearly state the entity's procedures for responding to suspected or known security incidents? [assessment_10]
- [ ] **Adherence to Data Breach Notification Laws and Policies**: Does the entity's information sharing policy clearly state the entity's procedures for adhering to data breach notification laws or policies? [assessment_11]

Issuance Criteria:
yes(ALL)

Information Sharing Policy: Information Retention and Destruction

- [ ] **Review for Validation or Purging of Data**: Does the entity's information sharing policy clearly state the entity's review schedule for validating or purging information and the periodic basis for this and/or reference to the applicable law(s)? [assessment_01]
- [ ] **Retention and Destruction policies and Methods**: Does the entity's information sharing policy clearly state whether the entity has a retention and destruction policy, what methods the entity employs to remove or destroy, and whether law or policy is referenced, if applicable? (Note: A retention and destruction policy should be provided for all PHI databases/records held by the entity.) [assessment_02]

- [ ] **Scheduling, Recording, and Notification of Data Purging**: Does the entity's information sharing policy clearly state whether a record is kept of dates when information is to be removed (purged) if not validated prior to the end of its period and whether notification is given prior to removal (for example, an autogenerated system prompt to entity personnel that a record is due for review and validation or purge)? [assessment_03]
- [ ] **Confirmation and Log of Deletions**: Does the entity's information sharing policy clearly state whether a confirmation of the deletion is kept, including a log of the deletion (e.g., date of deletion)? [assessment_04]

Issuance Criteria:
yes(ALL)

Information Sharing Policy: Training

- [ ] **Personnel Required to be Trained**: Does the entity's information sharing policy clearly state what personnel the entity requires to participate in training programs regarding implementation of and adherence to the policy? [assessment_01]
- [ ] **Training Program Coverage**: Does the entity's information sharing policy clearly state what is covered by the training program (for example, purpose of the policy, substance and intent of the provisions of the policy, security requirements, impact of infractions, and possible penalties for violations)? [assessment_02]

Issuance Criteria:
yes(ALL)

PHI Privacy Policy: Governance and Oversight

- [ ] **Privacy Oversight**: Does the entity's PHI privacy policy clearly state whether the entity has a privacy oversight committee, team, or individual that is responsible for the development of the PHI privacy policy and/or that will routinely review and update the policy? [assessment_02]
- [ ] **Privacy Officer**: Does the entity's PHI privacy policy clearly state whether there is a designated and trained privacy officer (or privacy officer function) within the entity who will handle reported errors and violations and oversee the implementation of PHI privacy protections, and does the policy identify the title of the individual who will serve as the privacy officer, whether a full-time privacy officer position or the occupant of a different position, such as the assistant director or entity counsel, and provide the contact information for the privacy officer (for example, phone, Web site, e-mail, or U.S. mail address)? [assessment_03]
- [ ] **Responsibility for Enforcement and Sanctions**: Does the entity's PHI privacy policy clearly state who is responsible for ensuring that enforcement procedures and sanctions for noncompliance with the PHI privacy policy are adequate and enforced? [assessment_04]

Issuance Criteria:
yes(ALL)

Information Sharing Policy: Governance and Oversight

- [ ] **Primary Responsibility**: Does the entity's information sharing policy clearly state who has primary responsibility for the entity's overall operation, including the entity's information systems, information collection and retention procedures, coordination of personnel, and enforcement of policies, including privacy policies and which individual will ultimately be held accountable for the operation of the information system and for any problems or errors? [assessment_01]

Issuance Criteria:
yes(ALL)

PHI Privacy Policy: Information

- [ ] **Information Labeling**: Does the entity's PHI privacy policy clearly state whether the entity applies labels (by record, data set, or system of records) to the maximum extent feasible, to entity-originated PHI (or ensures that the PHI-providing entity has applied labels) to indicate to the accessing authorized information recipient that:
  - The information is "protected health information," including personally identifiable information on any individual regardless of citizenship or U.S. residency status?
  - The information has applicable limitations on access and sensitivity of disclosure, is subject to specific health information privacy or other similar restrictions and, if so, the nature of such restrictions?
  - The laws that restrict who can access information, how information can be used, and the retention or disclosure of certain types of information? [assessment_04]
- [ ] **Categorization Reevaluation**: Does the entity's information sharing policy clearly state the conditions that prompt the labels cited in 1 above to be reevaluated? [assessment_06]
- [ ] **Required Metadata and Labels**: Does the entity's PHI privacy policy clearly state whether the entity requires certain basic descriptive information (metadata tags or labels) to be entered and associated with each record, data set, or system of records containing PHI that will be accessed, used, and disclosed?
  - Basic information may include, where relevant and appropriate: the name of the PHI-providing entity, department, component, or subcomponent (if applicable).
  - If applicable, the name of the entity's information system from which the information is disseminated.
  - The date the information was collected (submitted) and, where feasible, the date its accuracy was last verified.
  - The title and contact information for the person to whom questions regarding the information, including its accuracy, should be directed. [assessment_07]

Issuance Criteria:
yes(ALL)

Information Sharing Policy: Information

- [ ] **Type of Information**: Does the entity's information sharing policy clearly state what information may be sought, retained, shared, disclosed or disseminated, by the entity and whether there are different policy provisions for different types of information (e.g., medical, mental health, and substance abuse information, as well as fact-based information databases)? [assessment_01]
- [ ] **Purpose for Use of Information**: Does the entity's information sharing policy clearly state the purpose(s) for which information may be sought, retained, shared, disclosed, or disseminated by the entity? [assessment_02]
- [ ] **Disallowed Information**: Does the entity's information sharing policy clearly state what information may not be sought, retained, shared, disclosed, or redisclosed by the entity (e.g., for reasons of discrimination)? [assessment_03]
- [ ] **Information Categorization**: Does the entity's information sharing policy clearly state whether the entity categorizes information (or ensures that the PHI-providing entity has categorized information) based on its nature (for example, conditions of supervision, medical, mental health, and substance abuse information), usability, and quality? [assessment_04]
- [ ] **Categorization Reevaluation**: Does the entity's information sharing policy clearly state the conditions that prompt the labels cited in 4 above to be reevaluated? [assessment_05]
- [ ] **Recording of Source**: Does the entity's information sharing policy clearly state whether the entity maintains a record of the source of the information sought and collected? [assessment_06]

Issuance Criteria:
yes(ALL)

PHI Privacy Policy: Information Quality Assurance

- [ ] **Procedure for Amending PHI**: Does the entity's PHI privacy policy clearly state, in the case of a HIPAA-covered entity, the entity's procedure for amending PHI if informed by another covered entity of a need to amend an individual's record? [assessment_06]

Issuance Criteria:
yes(ALL)

Information Sharing Policy: Information Quality Assurance

- [ ] **Procedures to Endure Data Quality**: Does the entity's information sharing policy clearly state whether the entity has established procedures and procedures (manual and electronic) to ensure the quality (for example, accurate, complete, current, verifiable, and reliable) of the information it

collects, maintains, and disseminates? [assessment_01]

- [ ] **Research of Alleged or Suspected Errors**: Does the entity's information sharing policy clearly state whether the entity researches alleged or suspected errors and deficiencies (or refers them to the PHI- providing agency) and how the entity responds to confirmed errors or deficiencies? [assessment_02]
- [ ] **Review for Bad Data**: Does the entity's information sharing policy clearly state when the entity reviews the quality of the information it originates and identifies data that may be inaccurate or incomplete, includes incorrectly merged information, is out of date, cannot be verified, has a questionable source, or lacks adequate context such that the rights of the individual may be affected, the entity's procedure for correction or destruction? [assessment_03]
- [ ] **Notification to Originating Agency in Case of Bad Data**: Does the entity's information sharing policy clearly state when the entity reviews the quality of the information it has received from an originating agency and identifies data that may be inaccurate or incomplete, includes incorrectly merged information, is out of date, cannot be verified, has a questionable source, or lacks adequate context such that the rights of the individual may be affected, whether the entity notifies the originating agency or the originating agency's privacy officer and the method used to notify the agency (written, telephone, or electronic notification)? [assessment_04]
- [ ] **Notification to External Agency in Case of Bad Data**: Does the entity's policy clearly state when the entity reviews the quality of the PHI it has provided to an external agency and identifies data that may be inaccurate or incomplete, includes incorrectly merged information, is out of date, cannot be verified, has a questionable source, or lacks adequate context such that the rights of the individual may be affected, whether the entity notifies the external agency? [assessment_05]

Issuance Criteria:
yes(ALL)

PHI Privacy Policy: Accountability and Enforcement

- [ ] **Information System Transparency: Policy Posted on Web Site**: Does the entity's PHI privacy policy clearly state, if your entity is a HIPAA-covered entity, whether the entity posts its PHI privacy policy on the entity's Web site? [assessment_01-02]
- [ ] **Information System Transparency: Requirements Notification to Patients**: Does the entity's PHI privacy policy clearly state, if your entity is a federally assisted program, whether the entity provides a notice to patients of federal confidentiality requirements (e.g., substance abuse information, 42 CFR Part 2)? [assessment_01-03]
- [ ] **Information System Transparency: Policy Complaint Process**: Does the entity's PHI privacy policy clearly state whether the entity has a process for individuals to make complaints concerning the entity's policies, procedures, and privacy practices if the individual feels that a violation of HIPAA or 42 CFR Part 2 has occurred? [assessment_01-04]
- [ ] **Accountability: Procedures for Evaluation of User Compliance**: Does the entity's PHI privacy policy clearly state the procedures and practices the entity follows to enable evaluation of user compliance with information access requirements, the entity's PHI privacy policy, and applicable

law? [assessment_02-03]

- [ ] **Accountability: Consent Authorization Retention Periods and Audit Trails Thereof**: Does the entity's PHI privacy policy clearly state the entity's retention period for patient consent authorizations, and whether audits are completed to ensure that appropriate consent authorizations are maintained and current? [assessment_02-05]
- [ ] **Enforcement: Authorization Qualifications for Access and Sanctions for Violations**: Does the entity's PHI privacy policy clearly state the entity's policy with regard to the qualifications and number of participating agency personnel authorized to access PHI, and the additional sanctions the entity may utilize for violations of the entity's PHI privacy policy? [assessment_03-02]

Issuance Criteria:
yes(ALL)

Information Sharing Policy: Accountability and Enforcement

- [ ] **Information System Transparency: Publicly Available Policy**: Does the entity's information sharing policy clearly state whether the entity's policy is available to the public (for example, provided to the public for review, made available upon request, and/or posted on the entity's Web site—include Web address)? [assessment_01-01]
- [ ] **Information System Transparency: Point of Contact for Inquiries and Complaints**: Does the entity's information sharing policy clearly state whether the entity has a point of contact (position/title) for handling inquiries or complaints, and whether the contact information for this individual (for example, phone, Web site, e-mail, or U.S. mail address) is provided? [assessment_01-05]
- [ ] **Accountability: User-Identified Access and Logging Thereof**: Does the entity's information sharing policy clearly state whether access (e.g., electronic or hard-copy access) to the entity's data identifies the user, and whether the identity of the user is retained in the audit log? [assessment_02-01]
- [ ] **Accountability: Data Log and Audit Trail**: Does the entity's information sharing policy clearly state whether a log (electronic or paper) is kept of accessed and disseminated entity-held data, and whether an audit trail is maintained? [assessment_02-02]
- [ ] **Accountability: Mechanism for Reporting Errors and Violations**: Does the entity's information sharing policy clearly state whether the entity has a mechanism for personnel to report errors and suspected or confirmed violations of entity privacy policies related to PHI? [assessment_02-04]
- [ ] **Accountability: Auditing Entity**: Does the entity's information sharing policy clearly state whether audits are completed by an independent third party or a designated representative of the entity? [assessment_02-06]
- [ ] **Accountability: Review and Update of Policy Provisions**: Does the entity's information sharing policy clearly state how often the entity reviews and updates the provisions contained within the policy (recommendation is annually), and whether a record is kept of all changes to entity information sharing policies, including security provisions and procedures and, if so, the entity's retention period for such documentation? [assessment_02-07]

- [ ] **Enforcement: Enforcement Procedures for Noncompliance**: Does the entity's information sharing policy clearly state the procedures for enforcement if entity personnel, a participating agency, or an authorized user is suspected of being or has been found to be in noncompliance with the provisions of the entity's information sharing policy? [assessment_03-01]

Issuance Criteria:
yes(ALL)

Authorization Revocation

- [ ] **Revocation by Consenting Individual**: Has the individual revoked the consent authorization? [assessment_01]
- [ ] **Action in Reliance of Consent**: Has the covered entity has taken action in reliance the consent authorization? [assessment_02]
- [ ] **Insurance Coverage and Contest of Claim** : Was the consent authorization obtained as a condition of obtaining insurance coverage and does other law provides the insurer with the right to contest a claim under the policy or the policy itself? [assessment_03]

Issuance Criteria:
no(assessment_01) OR (yes(assessment_02) OR yes(assessment_03))

HIPAA Consent Authorization Form Requirements - Elements

- [ ] **Information to be Disclosed**: Does the authorization include a description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion? [assessment_01]
- [ ] **Identification of Persons Authorized to Request or Disclose**: Does the authorization include the name or other specific identification of the person(s) or class of persons authorized to make the requested use or disclosure? [assessment_02]
- [ ] **Identification of Persons Authorized to Receive Disclosure**: Does the authorization include the name or other specific identification of the person(s) or class of persons to whom the covered entity may make the requested use or disclosure? [assessment_03]
- [ ] **Purpose of Use or Disclosure**: Does the authorization include a description of each purpose of the requested use or disclosure. Note: The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose? [assessment_04]
- [ ] **Expiration Conditions Specified**: Does the authorization include an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. Note: The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of PHI for research, including for the creation and maintenance of a research database or research repository? [assessment_05]
- [ ] **Signature of Person Authorizing Disclosure**: Does the authorization include the signature of the

individual and date signed. Note: If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual also must be provided? [assessment_06]

HIPAA Consent Authorization Form Requirements - Notice Statements

- [ ] **Notice of Right to Revoke**: Does the authorization contain statements adequate to place the individual on notice of the individual's right to revoke the authorization in writing, and either:
  - The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or
  - To the extent that the exceptions to the right to revoke are included in the notice required by HIPAA's notice of privacy practices for PHI, as per § 164.520, a reference to the covered entity's notice? [assessment_07]
- [ ] **Notice of Ability to Condition on Authorization**: Does the authorization contain statements adequate to place the individual on notice of the ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the authorization, by stating either:
  - The covered entity may not condition treatment, payment, enrollment, or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations applies; or
  - The consequences to the individual of a refusal to sign the authorization when the covered entity can, per § 164.508(b)(4), condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization? [assessment_08]
- [ ] **Notice of Potential Redisclosure**: Does the authorization contain statements adequate to place the individual on notice of the potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer to be protected? [assessment_09]

Issuance Criteria:
yes(ALL)

---

42 CFR Part 2 Consent Authorization Form Requirements - Elements

- [ ] **Identification of Entity Making the Disclosure**: Does the written consent to a disclosure include the specific name or general designation of the program or person permitted to make the disclosure? [assessment_01]
- [ ] **Identification of Entity Receiving the Disclosure**: Does the written consent to a disclosure include the name or title of the individual or the name of the organization to which disclosure is to be made. Note: The authorization has to specifically state the name of the provider or the general designation of the treatment center (e.g., Shady Grove Substance Abuse Center)? [assessment_02]
- [ ] **Patient Name**: Does the written consent to a disclosure include the name of the patient? [assessment_03]
- [ ] **Purpose of Disclosure**: Does the written consent to a disclosure include the purpose of the disclosure? [assessment_04]

- [ ] **Kind and Amount to be Disclosed**: Does the written consent to a disclosure include how much and what kind of information is to be disclosed? [assessment_05]
- [ ] **Signature of Authorizing Person**: Does the written consent to a disclosure include the signature of the patient and, when required for a patient who is a minor, the signature of a person authorized to give consent under § 2.14; or, when required for a patient who is incompetent or deceased, the signature of a person authorized to sign under § 2.15 in lieu of the patient? [assessment_06]
- [ ] **Date Consent Form Signed**: Does the written consent to a disclosure include the date on which the consent is signed? [assessment_07]
- [ ] **Expiration Conditions Specified**: Does the written consent to a disclosure include the date, event, or condition upon which the consent will expire if not revoked before. This date, event, or condition must ensure that the consent will last no longer than reasonably necessary to serve the purpose for which it is given? [assessment_08]

42 CFR Part 2 Consent Authorization Form Requirements - Notice Statements

- [ ] **Notice of Potential Revocation**: Does the authorization contain statements adequate to place the individual on notice that the consent is subject to revocation at any time, except to the extent that the program or person making the disclosure has already acted in reliance on it. Acting in reliance includes the provision of treatment services in reliance on a valid consent to disclose information to a third-party payer? [assessment_09]
- [ ] **Notice of Subsequent Redisclosure**: Under 42 CFR Part 2, a single consent form can authorize a disclosure of information about a patient to one recipient, and simultaneously authorize that recipient to redisclose that information to any additional entity or entities (such as other affiliated health-care providers identified in the consent form), provided that the purpose for the disclosure is the same. Does the authorization contain the following required statement prohibiting redisclosure, so that each subsequent recipient of that information is notified of the prohibitions on redisclosure?

> *This notice covers the disclosure of information to you concerning a client in alcohol/drug treatment, made to you with the consent of such client. This information has been disclosed to you from records protected by federal confidentiality rules (42 C.F.R. Part 2). The federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 C.F.R. Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The federal rules restrict any use of the information to criminally investigate or prosecute any substance abuse patient. [assessment_10]*

Issuance Criteria:
yes(ALL)

HIPPA Defective Authorizations

- [ ] **Expiration**: Has the expiration date passed or does the covered entity know that the expiration event has occurred? [assessment_01]
- [ ] **Completeness**: Has the authorization been filled out completely, with respect to required elements? [assessment_02]
- [ ] **Revocation**: Does covered entity know that the authorization has been revoked? [assessment_03]
- [ ] **False Information**: Is any material information in the authorization known by the covered entity to be false? [assessment_04]

Compound Authorizations

- [ ] **Compound Authorizations**: Is the authorization combined with any other document to create a compound authorization? [assessment_05]
- [ ] **Research Studies**: Is the authorization for a research study and is combined with any other type of written permission for the same research study, including another authorization for the use or disclosure of PHI for such research or a consent to participate in such research? [assessment_06]
- [ ] **Psychotherapy Notes**: Is the authorization for a use or disclosure of psychotherapy notes and is combined only with another authorization for a use or disclosure of psychotherapy notes? [assessment_07]
- [ ] **Psychotherapy Notes**: Is the authorization for a use or disclosure of psychotherapy notes and is combined with any other such authorization under this Trustmark Definition? [assessment_08]

Prohibition on Conditioning of Authorizations

- [ ] **Conditioned Authorizations**: Does the covered entity condition the provision treatment, payment, enrollment in a health plan, or eligibility for benefits to an individual on a Consent Authorization? [assessment_09]
- [ ] **Research-Related Treatment**: Is a covered health-care provider conditioning the provision of research-related treatment on a consent authorization for the use or disclosure of PHI for such research? [assessment_10]
- [ ] **Health Care Plan Enrollment and Benefits**: Is a covered health-care provider conditioning health plan enrollment or eligibility for benefits on a consent authorization requested by the health plan *prior* to an individual's enrollment in the health plan, and the authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk-rating determinations, and the authorization is not for a use or disclosure of psychotherapy notes? [assessment_11]
- [ ] **PHI-Creation-Specific Health Care**: Is the health care being provisioned solely for the purpose of creating PHI for disclosure to a third party on provision of an authorization for the disclosure of the PHI to such third party? [assessment_12]

Issuance Criteria:
(no(assessment_01) AND yes(assessment_02) AND no(assessment_03) AND no(assessment_04)) AND (!yes(assessment_05) OR yes(assessment_06) OR yes(assessment_07)) AND (!yes(assessment_09) OR yes(assessment_10 OR yes(assessment_11) OR yes(assessment_12))

HIPAA Consent Authorization Form Requirements - Elements

- [ ] **Expiration**: Has the consent form expired? [assessment_01]
- [ ] **Revocation**: Is the consent form known to have been revoked? [assessment_02]
- [ ] **Material Falsehood**: Is the consent form known, or through a reasonable effort could be known, by the person holding the records to be materially false? [assessment_03]

Issuance Criteria:
no(ALL)

Valid HIPAA Business Associate

- [ ] **Not a HIPAA Covered Entity**: Is the organization a HIPAA covered Entity? [assessment_01]
- [ ] **Provides Covered Functions or Activities**: Does the organization perform any of the following functions or activities that involve the use or disclosure of PHI on behalf of a covered entity? (Claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, or repricing.) [assessment_02]
- [ ] **Provides Covered Services**: Does the organization provide any of the following services that involve the use or disclosure of PHI to a covered entity? (Legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial.) [assessment_03]

Issuance Criteria:
no(assessment_01) and (yes(assessment_02) or yes(assessment_03))

Contractual Agreements with HIPPA-Covered Entities

- [ ] **Agreement to Limit Disclosure**: Do the organization's contracts contain language concerning the Business Associate agreeing to not use or disclose PHI other than as permitted or required by the Agreement or as Required by Law? [assessment_01]
- [ ] **Safeguards to Limit Disclosure**: Do the organization's contracts contain language concerning the Business Associate agreeing to use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by the Agreement? [assessment_02]
- [ ] **Agreement to Comply with Requirements**: Do the organization's contracts contain language concerning the Business Associate agreeing to comply with applicable security, administrative, physical, and technical safeguards requirements at both the State and Federal levels? [assessment_03]
- [ ] **Data Breach Notification**: Do the organization's contracts contain language concerning notification of HIPAA-Covered Entity in case of data breach? [assessment_04]
- [ ] **Data Breach Damage Mitigation**: Do the organization's contracts contain language concerning mitigating damages in case of data breach? [assessment_05]
- [ ] **Outside Use Notification**: Do the organization's contracts contain language concerning

notification to HIPAA-Covered Entity of uses outside the scope of the agreement? [assessment_06]

- [ ] **Limits on Passing Data**: Do the organization's contracts contain language limiting the passing on of data only with the same agreement bound to agents or sub-contractors? [assessment_07]
- [ ] **Data Availability on Entity Direction**: Do the organization's contracts contain language concerning agreements to make data available on direction of HIPAA-Covered Entity? [assessment_08]
- [ ] **Data Update on Entity Direction**: Do the organization's contracts contain language concerning agreements to update data on direction of HIPAA-Covered Entity? [assessment_09]
- [ ] **Assessements Policy**: Do the organization's contracts contain language concerning the availability of policies, etc, to HHS to allow for assessments? [assessment_10]
- [ ] **Documentation of Disclosures**: Do the organization's contracts contain language concerning documenting disclosures for purpose of accounting of those disclosures? [assessment_11]
- [ ] **Providing of Documentation of Disclosures**: Do the organization's contracts contain language concerning providing documentations of disclosures for the purpose of accounting of those disclosures? [assessment_12]
- [ ] **Allowed Purposes**: Do the organization's contracts contain language specifying purposes for which PHI may be disclosed or alternately refer to a services agreement providing such information? [assessment_13]
- [ ] **Use and Disclosure Provisions**: Do the organization's contracts contain language concerning specific use and disclosure provisions? [assessment_14]
- [ ] **Communication of Privacy Practices and Restrictions**: Do the organization's contracts contain language concerning provisions for HIPAA-Covered Entity to inform Business Associate of privacy practices and restrictions, dependent on specific business arrangements? [assessment_15]
- [ ] **Permissible Entity Requests**: Do the organization's contracts contain language concerning descriptions of permissible requests by HIPAA-Covered Entity? [assessment_16]
- [ ] **Term of Agreement**: Do the organization's contracts contain language concerning the term of the agreement, including effective date and date or conditions of termination? [assessment_17]
- [ ] **Termination Procedures**: Do the organization's contracts contain language concerning termination procedures when termination for cause occurs? [assessment_18]
- [ ] **Post-Termination Procedures**: Do the organization's contracts contain language concerning post-termination procedures, including subsequent destruction of PHI? [assessment_19]

Issuance Criteria:
yes(ALL)

Redress Policy

- [ ] **Disclosure Notice**: Does the organization's Redress Policy disclose to individual about whom the information was gathered the conditions under which the entity will disclose PHI information? [assessment_01]
- [ ] **Disclosure Record**: Does the organization keep a record of all requests and of what information is disclosed to an individual? [assessment_02]

- [ ] **Disclosure Exceptions**: Does the organization document exceptions when the individual about whom the information was gathered is not notified? This includes whether the entity refers the individual to the agency originating the information? [assessment_03]
- [ ] **Data Amendments**: Does the organization perform any of the following functions or activities that involve the use or disclosure of PHI on behalf of a covered entity? (Claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, or repricing.) [assessment_04]
- [ ] **Data Amendment Point of Contact**: Does the organization provide any of the following services that involve the use or disclosure of PHI to a covered entity? (Legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial.) [assessment_05]
- [ ] **Data Amendment Retention Record**: Does the organization provide any of the following services that involve the use or disclosure of PHI to a covered entity? (Legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial.) [assessment_06]
- [ ] **Data Amendment Point of Contact**: Does the organization provide a point of contact for handling individuals' requests for amendments of PHI? [assessment_07]
- [ ] **Data Amendment Procedure**: Does the organization have a procedure for handling individuals' requests for correction (or amendments) involving information that the entity can change because it originated the information? [assessment_08]
- [ ] **Data Amendment Record**: Does the organization maintain a record of requests for corrections (amendments) [assessment_09]
- [ ] **Appeal Conditions**: Does the organization document the conditions under which the entity may deny an individual’s request for access or correction (amendment)? [assessment_10]
- [ ] **Appeal Procedure**: If requests for access or corrections (amendments) are denied, does the entity have a procedure for appeal (or review)? [assessment_11]

Issuance Criteria:
yes(ALL)

Corrections and Reentry: Protected Health Information Privacy Framework for Information Sharing Trust Interoperability Profile

URI:
http://ncsc.org/trustmarks/trustmark-definitions/corrections-and-reentry/1.0/

Description:
This Trust Interoperability Profile defines requirements for a Protected Health Information Privacy Framework for Information Sharing for Corrections and Reentry.

References

Trustmark Definition Requirements

- None

Trust Interoperability Profiles

- PHI Privacy Policy TIP [TIP_01]
- Consent Authorizations Profile TIP [TIP_02]
- Contractual Agreements Profile TIP [TIP_03]

Trust Expression:

TIP_01 AND TIP_02 AND TIP_03

PHI Privacy Policy Trust Interoperability Profile

URI:
http://ncsc.org/trustmarks/trustmark-definitions/PHI-privacy-policy/PHI-policy-TIP/1.0/

Description:
This Trust Interoperability Profile specifies requirements for creating a PHI Privacy Policy for exchanging Protected Health Information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and 42 CFR Part 2.

References

Trustmark Definition Requirements

- Policy: Purpose Statement TD [Generic-A-TD]
- Policy: Policy Applicability and Legal Compliance TD [Generic-B-TD]
- Policy: Definitions TD [Generic-D-TD]
- Information Sharing Policy: Acquiring and Receiving Information TD [IS-F-TD]
- PHI Privacy Policy: Program Evaluation and Research TD [PHI-H-TD]
- Information Sharing Policy: Merging Records TD [IS-I-TD]
- PHI Privacy Policy: Use and Disclosure TD [PHI-J-TD]
- Redress Policy TD [Redress-TD]
- Information Sharing Policy: Information Security Safeguards TD [IS-L-TD]
- Information Sharing Policy: Information Retention and Destruction TD [IS-M-TD]
- Information Sharing Policy: Training TD [IS-O-TD]

Trust Interoperability Profiles

- PHI Privacy Policy: Governance and Oversight (TIP) TIP [PHI-C-TIP]
- PHI Privacy Policy: Information (TIP) TIP [PHI-E-TIP]
- PHI Privacy Policy: Information Quality Assurance (TIP) TIP [PHI-G-TIP]
- PHI Privacy Policy: Accountability and Enforcement (TIP) TIP [PHI-N-TIP]

Trust Expression:

Generic-A-TD AND Generic-B-TD AND PHI-C-TIP AND Generic-D-TD AND PHI-E-TIP AND IS-F-TD AND PHI-G-TIP AND PHI-H-TD AND IS-I-TD AND PHI-J-TD AND Redress-TD AND IS-L-TD AND IS-M-TD AND PHI-N-TIP AND IS-O-TD

Policy: Purpose Statement Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/PHI-privacy-policy/generic-policy-purpose-statement/1.0/

Description:
This Trustmark Definition defines requirements for creating the Purpose Statement aspects of a generic Policy.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

Policy: Purpose Statement

Description: The policy MUST contain the required Purpose sections.

- **Policy Purpose**: Does the entity's policy clearly state the purpose of establishing a privacy, civil rights, and civil liberties protection policy (i.e., what does the entity hope to accomplish in adopting this policy)? [assessment_01]

Issuance Criteria:
yes(ALL)

Policy: Policy Applicability and Legal Compliance Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/PHI-privacy-policy/generic-policy-policy-applicability-and-legal-compliance/1.0/

Description:
This Trustmark Definition defines requirements for creating the Policy Applicability and Legal Compliance aspects of a generic Policy.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

Policy: Policy Applicability and Legal Compliance

Description: The policy MUST contain the required Policy Applicability and Legal Compliance sections.

- **Subject to Policy**: Does the entity's policy clearly state who is subject to the policy (who must comply with the policy; for example, entity personnel, participating agencies, and private contractors)? [assessment_01]
- **Policy Dissemination**: Does the entity's policy clearly state the method(s) by which the policy is made available to personnel, participating entities, and individual users (for example, in print, online, etc.) and whether the entity requires personnel, participating entities, and individual users to acknowledge receipt of the policy and agreement to comply with the policy in writing? [assessment_02]
- **Requirement of Law Compliance**: Does the entity's policy clearly state that personnel and participating information-originating and user agencies must be in compliance with all applicable law protecting privacy, civil rights, and civil liberties in the gathering and collection, use, analysis, retention, destruction, sharing, disclosure, and dissemination of medical, mental health, and substance abuse information and list the primary laws with which personnel and participating users must comply? [assessment_03]
- **Internal Policies in Compliance with Laws**: Does the entity's policy clearly state whether the entity's internal operating policies are in compliance with all applicable law protecting privacy, civil rights, and civil liberties in the gathering and collection, use, analysis, retention, destruction, sharing, disclosure, and dissemination of medical, mental health, and substance abuse information, and are the laws with which internal operation policies must be in compliance cited in the privacy policy? [assessment_04]

Issuance Criteria:
yes(ALL)

Policy: Definitions Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/PHI-privacy-policy/generic-policy-definitions/1.0/

Description:
This Trustmark Definition defines requirements for creating the Definitional aspects of a generic Policy.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

Policy: Definitions

Description: The policy MUST contain the required Definitions sections.

- **Term Definitions**: Does the entity's policy clearly state the key words or phrases (and definitions) that are regularly used in the policy for which the entity wants to specify particular meanings? [assessment_01]

Issuance Criteria:
yes(ALL)

Information Sharing Policy: Acquiring and Receiving Information Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/PHI-privacy-policy/IS-policy-acquiring-and-receiving-information/1.0/

Description:
This Trustmark Definition defines requirements for creating the Acquiring and Receiving Information aspects of an Information Sharing Policy.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

Information Sharing Policy: Acquiring and Receiving Information

Description: The policy MUST contain the required Acquiring and Receiving Information sections.

- **Sharing Agencies Adhere to Laws and Policies**: Does the entity's information sharing policy clearly state whether the agencies that access your entity's PHI and/or share PHI with your entity ensure that they will adhere to applicable laws and policies? [move to PHI?] [assessment_01]
- **Compliance Assurance for Commercial Database Providers**: Does the entity's information sharing policy clearly state whether the entity contracts with commercial databases and, if so, how the entity ensures that the commercial database company is in legal compliance in its information-gathering techniques? [assessment_02]

Issuance Criteria:
yes(ALL)

PHI Privacy Policy: Program Evaluation and Research Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/PHI-privacy-policy/PHI-policy-program-evaluation-and-research/1.0/

Description:
This Trustmark Definition defines requirements for creating the Program Evaluation and Research aspects of a PHI Privacy Policy for exchanging Protected Health Information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and 42 CFR Part 2.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

PHI Privacy Policy: Program Evaluation and Research

Description: The policy MUST contain the required Program Evaluation and Research sections.

- **Authorization to Analyze Deidentified PHI**: Does the entity's PHI privacy policy clearly state who is authorized (position/title, credentials, etc.) to analyze deidentified PHI for evaluation and research purposes? [assessment_01]
- **Determination of Which Deidentified PHI to Analyze**: Does the entity's PHI privacy policy clearly state what deidentified PHI is analyzed? [assessment_02]
- **Purpose for Analyzing Deidentified PHI**: Does the entity's PHI privacy policy clearly state for what purpose(s) is the deidentified PHI analyzed? [assessment_03]

Issuance Criteria:
yes(ALL)

Information Sharing Policy: Merging Records Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/PHI-privacy-policy/IS-policy-merging-records/1.0/

Description:
This Trustmark Definition defines requirements for creating the Merging Records aspects of an Information Sharing Policy.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

Information Sharing Policy: Merging Records

Description: The policy MUST contain the required Merging Records sections.

- **Persons Authorized to Merge Records**: Does the entity's information sharing policy clearly state who is authorized (position/title, credentials, etc.) to merge records? [assessment_01]
- **Criteria for Merging**: Does the entity's information sharing policy clearly state what matching criteria the entity requires when attempting to merge information from multiple records allegedly about the same individual? In other words, when two records are compared for possible merger, are there certain attributes (name, date of birth, social security number, etc.) that must match, or is there a minimum number of attributes (for example, two out of five) that must match to link the two records as relating to the same person? [assessment_02]
- **Associating Records not Meeting Merge Criteria**: Does the entity's information sharing policy clearly state the entity's procedure for associating records, if the criteria specified in 2 above are not met? (Note: If the entity does not merge or associate records that have partial matches, then the policy should so state.) [assessment_03]

Issuance Criteria:
yes(ALL)

PHI Privacy Policy: Use and Disclosure Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/PHI-privacy-policy/PHI-policy-use-and-disclosure/1.0/

Description:
This Trustmark Definition defines requirements for creating the Use and Disclosure aspects of a PHI Privacy Policy for exchanging Protected Health Information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and 42 CFR Part 2.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

PHI Privacy Policy: Use and Disclosure

Description: The policy MUST contain the required Use and Disclosure sections.

- **Controlled Actions and Permissions of PHI Recipients**: Does the entity's PHI privacy policy clearly state what types of information recipient actions and permissions are controlled by the entity's access or dissemination limitations? Best practice: It is suggested that entities specify their method for identifying information recipient actions and permissions in their privacy policies. (Note: Information recipient actions and permissions are often used to identify entities and individuals with a need and right to know particular information; to access case management information (including medical, mental health, and/or substance abuse information); access nonpersonally identifiable information only; or to identify who is authorized to submit or modify particular records or record sets, to have read-only access or to be authorized to add/modify/delete records, or to be authorized to grant privileges.) [assessment_01]
- **Implemented Limits on Disclosure**: Does the entity's PHI privacy policy clearly state what limitations the entity has implemented to limit or restrict disclosure of PHI? [assessment_02]
- **Conditions and Credentials for Access and Disclosure and Audit Trails Thereof**: Does the entity's PHI privacy policy clearly state the conditions and credentials by which access to and disclosure of PHI records retained by the entity will be provided within the entity or in other governmental agencies, and whether an audit trail is kept of access to and disclosure of PHI retained by the entity (e.g., dissemination logs, algorithms)? [assessment_03]
- **Conditions Requiring Individual Consent Authorization**: Does the entity's PHI privacy policy clearly state the conditions by which access to and disclosure of PHI retained by the entity are not permitted without an individual consent authorization? [assessment_04]
- **Released Individual Restriction and Nondisclosure Requests**: Does the entity's PHI privacy policy clearly state whether the entity permits released individuals (those who are no longer in lawful custody) to request that the entity restrict the use and disclosure of the individuals' PHI retained by the entity? [assessment_05]
- **Disclosure for Released Individuals**: Does the entity's PHI privacy policy clearly state, for individuals who are released from custody (for example, on probation or parole), the conditions by which the entity may use or disclose PHI without the individuals' written consent authorization? [assessment_06]
- **Originator Approval Required**: Does the entity's PHI privacy policy clearly state whether participating agencies that access information from the entity are required to obtain approval from the originator of the information prior to further dissemination or to follow the disclosure or redisclosure law applicable to the originating agency, and, if the information is substance abuse information, does the entity provide the required 42 CFR Part 2 notice covering the disclosure of such information, along with any such disclosure of the substance abuse information? [assessment_07]
- **Conditions for Medical/Mental Health/Behavioral Health Release and Audit Trails Thereof**: Does the entity's PHI privacy policy clearly state the conditions under which access to and disclosure of PHI records retained by the entity will be provided to those responsible for medical, mental health and/or behavioral health, including substance use services, and whether an audit trail

is kept of access to and disclosure of information retained by the entity (e.g., dissemination logs, algorithms)? [assessment_08]

- **Conditions for Public Release and Audit Trails Thereof**: Does the entity's PHI privacy policy clearly state under what circumstances and what legal authority will access to and disclosure of a record be provided to a member of the public in response to an information request, and whether these circumstances are described in the entity's redress policy, and whether an audit trail is kept of access to and disclosure of information retained by the entity without the audit trail constituting an impermissible collection of information of a member of the public (e.g., dissemination logs, algorithms)? (Note: This does not apply to circumstances in which an entity chooses to provide nonsensitive information to the public or to provide sensitive information in accordance with entity policy in response to an emergency situation.) [assessment_09]
- **Conditions for Specific Release and Audit Trails Thereof**: Does the entity's PHI privacy policy clearly state the conditions under which release of information retained by the entity can be made for specific purposes or to specific persons, and whether an audit trail is kept showing how those conditions were met? [assessment_10]
- **Disallowed Entities and Circumstances**: Does the entity's PHI privacy policy clearly state under what circumstances and to whom the entity will not disclose PHI records? [assessment_11]
- **Categories Not Ordinarily Public**: Does the entity's PHI privacy policy clearly state the categories of records that ordinarily will not be provided to the public pursuant to applicable legal authority, and citations to applicable legal authority for each stated category? [assessment_12]
- **Existence Confirmation to Ineligible Entities**: Does the entity's PHI privacy policy clearly state the entity's policy on confirming the existence or nonexistence of information to persons or agencies that are not eligible to receive the information? [assessment_13]

Issuance Criteria:
yes(ALL)

Redress Policy Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/contractual-agreements/Redress-Policy/1.0/

Description:
This Trustmark Definition defines conformance for an organization having a Redress Policy.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

Redress Policy

Description: The organization MUST have an acceptable Redress Policy.

- **Disclosure Notice**: Does the organization's Redress Policy disclose to individual about whom the information was gathered the conditions under which the entity will disclose PHI information? [assessment_01]
- **Disclosure Record**: Does the organization keep a record of all requests and of what information is disclosed to an individual? [assessment_02]
- **Disclosure Exceptions**: Does the organization document exceptions when the individual about whom the information was gathered is not notified? This includes whether the entity refers the individual to the agency originating the information? [assessment_03]
- **Data Amendments**: Does the organization perform any of the following functions or activities that involve the use or disclosure of PHI on behalf of a covered entity? (Claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, or repricing.) [assessment_04]
- **Data Amendment Point of Contact**: Does the organization provide any of the following services that involve the use or disclosure of PHI to a covered entity? (Legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial.) [assessment_05]
- **Data Amendment Retention Record**: Does the organization provide any of the following services that involve the use or disclosure of PHI to a covered entity? (Legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial.) [assessment_06]
- **Data Amendment Point of Contact**: Does the organization provide a point of contact for handling individuals' requests for amendments of PHI? [assessment_07]
- **Data Amendment Procedure**: Does the organization have a procedure for handling individuals' requests for correction (or amendments) involving information that the entity can change because it originated the information? [assessment_08]
- **Data Amendment Record**: Does the organization maintain a record of requests for corrections (amendments) [assessment_09]
- **Appeal Conditions**: Does the organization document the conditions under which the entity may deny an individual's request for access or correction (amendment)? [assessment_10]
- **Appeal Procedure**: If requests for access or corrections (amendments) are denied, does the entity have a procedure for appeal (or review)? [assessment_11]

Issuance Criteria:
yes(ALL)

Information Sharing Policy: Information Security Safeguards Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/PHI-privacy-policy/IS-policy-information-security-safeguards/1.0/

Description:
This Trustmark Definition defines requirements for creating the Information Security Safeguards aspects of an Information Sharing Policy.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

Information Sharing Policy: Information Security Safeguards

Description: The policy MUST contain the required Information Security Safeguards sections.

- **Designated Security Officer**: Does the entity's information sharing policy clearly state whether the entity has a designated information security officer, whether training is provided for the information security officer, and, if the role is a component of another position, whether the policy identifies the title of the position upholding security officer responsibilities? [assessment_01]
- **Safeguards for Data Security**: Does the entity's information sharing policy clearly state the entity's physical, procedural, and technical safeguards for ensuring the security of entity data? (Does the policy describe how the entity will protect the information from unauthorized access, modification, theft, sabotage, or destruction [whether internal or external] resulting from natural or human-caused disasters or intrusions with, for example, procedures, practices, system protocols, use of software, information technology tools, process for data backups, and physical security measures?) [assessment_02]
- **Secure Format and Storage Environment**: Does the entity's information sharing policy clearly state the requirements that ensure that the information will be stored in a secure format and a secure environment? [assessment_03]
- **Assessment of Risks and Vulnerabilities of Held PHI**: Does the entity's information sharing policy clearly state if the entity is a HIPAA-covered entity, whether the entity has conducted an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the entity? [assessment_04]
- **Credentials for Authorized Access**: Does the entity's information sharing policy clearly state the required credentials of entity personnel authorized to have access to entity information? [assessment_05]
- **User-Identified Access**: Does the entity's information sharing policy clearly state whether electronic access to entity data identifies the user? [assessment_06]
- **Access Log and Audit Trail**: Does the entity's information sharing policy clearly state whether a log is kept of accessed and disseminated entity data, and whether an audit trail is maintained? [assessment_07]
- **Inactive Session Termination**: Does the entity's information sharing policy clearly state whether the entity has electronic procedures for terminating an electronic session after a period of inactivity? [assessment_08]
- **Risk and Vulnerability Assessments Separate from Public Data**: Does the entity's information sharing policy clearly state whether risk and vulnerability assessments (if maintained) are stored separately from publicly available data? [assessment_09]
- **Response to Security Incidents**: Does the entity's information sharing policy clearly state the entity's procedures for responding to suspected or known security incidents? [assessment_10]
- **Adherence to Data Breach Notification Laws and Policies**: Does the entity's information sharing policy clearly state the entity's procedures for adhering to data breach notification laws or policies? [assessment_11]

Issuance Criteria:
yes(ALL)

Information Sharing Policy: Information Retention and Destruction Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/PHI-privacy-policy/IS-policy-information-retention-and-destruction/1.0/

Description:
This Trustmark Definition defines requirements for creating the Information Retention and Destruction aspects of an Information Sharing Policy.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

Information Sharing Policy: Information Retention and Destruction

Description: The policy MUST contain the required Information Retention and Destruction sections.

- **Review for Validation or Purging of Data**: Does the entity's information sharing policy clearly state the entity's review schedule for validating or purging information and the periodic basis for this and/or reference to the applicable law(s)? [assessment_01]
- **Retention and Destruction policies and Methods**: Does the entity's information sharing policy clearly state whether the entity has a retention and destruction policy, what methods the entity employs to remove or destroy, and whether law or policy is referenced, if applicable? (Note: A retention and destruction policy should be provided for all PHI databases/records held by the entity.) [assessment_02]
- **Scheduling, Recording, and Notification of Data Purging**: Does the entity's information sharing policy clearly state whether a record is kept of dates when information is to be removed (purged) if not validated prior to the end of its period and whether notification is given prior to removal (for example, an autogenerated system prompt to entity personnel that a record is due for review and validation or purge)? [assessment_03]
- **Confirmation and Log of Deletions**: Does the entity's information sharing policy clearly state whether a confirmation of the deletion is kept, including a log of the deletion (e.g., date of deletion)? [assessment_04]

Issuance Criteria:
yes(ALL)

Information Sharing Policy: Training Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/PHI-privacy-policy/IS-policy-training/1.0/

Description:
This Trustmark Definition defines requirements for creating the Training aspects of an Information Sharing Policy.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

Information Sharing Policy: Training

Description: The policy MUST contain the required Training sections.

- **Personnel Required to be Trained**: Does the entity's information sharing policy clearly state what personnel the entity requires to participate in training programs regarding implementation of and adherence to the policy? [assessment_01]
- **Training Program Coverage**: Does the entity's information sharing policy clearly state what is covered by the training program (for example, purpose of the policy, substance and intent of the provisions of the policy, security requirements, impact of infractions, and possible penalties for violations)? [assessment_02]

Issuance Criteria:
yes(ALL)

PHI Privacy Policy: Governance and Oversight Trust Interoperability Profile

URI:
http://ncsc.org/trustmarks/trustmark-definitions/PHI-privacy-policy/PHI-policy-governance-and-oversight-TIP/1.0/

Description:
This Trust Interoperability Profile specifies requirements for creating the Governance and Oversight aspects of a PHI Privacy Policy for exchanging Protected Health Information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and 42 CFR Part 2.

References

Trustmark Definition Requirements

- PHI Privacy Policy: Governance and Oversight TD [PHI-C-TD]
- Information Sharing Policy: Governance and Oversight TD [IS-C-TD]

Trust Interoperability Profiles

- None

Trust Expression:

PHI-C-TD AND IS-C-TD

PHI Privacy Policy: Governance and Oversight Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/PHI-privacy-policy/PHI-policy-governance-and-oversight/1.0/

Description:
This Trustmark Definition defines requirements for creating the Governance and Oversight aspects of a PHI Privacy Policy for exchanging Protected Health Information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and 42 CFR Part 2.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

PHI Privacy Policy: Governance and Oversight

Description: The policy MUST contain the required Governance and Oversight sections.

- **Privacy Oversight**: Does the entity's PHI privacy policy clearly state whether the entity has a privacy oversight committee, team, or individual that is responsible for the development of the PHI privacy policy and/or that will routinely review and update the policy? [assessment_02]
- **Privacy Officer**: Does the entity's PHI privacy policy clearly state whether there is a designated and trained privacy officer (or privacy officer function) within the entity who will handle reported errors and violations and oversee the implementation of PHI privacy protections, and does the policy identify the title of the individual who will serve as the privacy officer, whether a full-time privacy officer position or the occupant of a different position, such as the assistant director or entity counsel, and provide the contact information for the privacy officer (for example, phone, Web site, e-mail, or U.S. mail address)? [assessment_03]
- **Responsibility for Enforcement and Sanctions**: Does the entity's PHI privacy policy clearly state who is responsible for ensuring that enforcement procedures and sanctions for noncompliance with the PHI privacy policy are adequate and enforced? [assessment_04]

Issuance Criteria:
yes(ALL)

Information Sharing Policy: Governance and Oversight Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/PHI-privacy-policy/IS-policy-governance-and-oversight/1.0/

Description:
This Trustmark Definition defines requirements for creating the Governance and Oversight aspects of an Information Sharing Policy.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

Information Sharing Policy: Governance and Oversight

Description: The policy MUST contain the required Governance and Oversight sections.

- **Primary Responsibility**: Does the entity's information sharing policy clearly state who has primary responsibility for the entity's overall operation, including the entity's information systems, information collection and retention procedures, coordination of personnel, and enforcement of policies, including privacy policies and which individual will ultimately be held accountable for the operation of the information system and for any problems or errors? [assessment_01]

Issuance Criteria:
yes(ALL)

PHI Privacy Policy: Information Trust Interoperability Profile

URI:
http://ncsc.org/trustmarks/trustmark-definitions/PHI-privacy-policy/PHI-policy-information-TIP/1.0/

Description:
This Trust Interoperability Profile specifies requirements for creating the Information aspects of a PHI Privacy Policy for exchanging Protected Health Information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and 42 CFR Part 2.

References

Trustmark Definition Requirements

- PHI Privacy Policy: Information TD [PHI-E-TD]
- Information Sharing Policy: Information TD [IS-E-TD]

Trust Interoperability Profiles

- None

Trust Expression:

PHI-E-TD AND IS-E-TD

PHI Privacy Policy: Information Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/PHI-privacy-policy/PHI-policy-information/1.0/

Description:
This Trustmark Definition defines requirements for creating the Information aspects of a PHI Privacy Policy for exchanging Protected Health Information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and 42 CFR Part 2.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

PHI Privacy Policy: Information

Description: The policy MUST contain the required Information sections.

- **Information Labeling**: Does the entity's PHI privacy policy clearly state whether the entity applies labels (by record, data set, or system of records) to the maximum extent feasible, to entity-originated PHI (or ensures that the PHI-providing entity has applied labels) to indicate to the accessing authorized information recipient that:
  - The information is "protected health information," including personally identifiable information on any individual regardless of citizenship or U.S. residency status?
  - The information has applicable limitations on access and sensitivity of disclosure, is subject to specific health information privacy or other similar restrictions and, if so, the nature of such restrictions?
  - The laws that restrict who can access information, how information can be used, and the retention or disclosure of certain types of information? [assessment_04]
- **Categorization Reevaluation**: Does the entity's information sharing policy clearly state the conditions that prompt the labels cited in 1 above to be reevaluated? [assessment_06]
- **Required Metadata and Labels**: Does the entity's PHI privacy policy clearly state whether the entity requires certain basic descriptive information (metadata tags or labels) to be entered and associated with each record, data set, or system of records containing PHI that will be accessed, used, and disclosed?
  - Basic information may include, where relevant and appropriate: the name of the PHI-providing entity, department, component, or subcomponent (if applicable).
  - If applicable, the name of the entity's information system from which the information is disseminated.
  - The date the information was collected (submitted) and, where feasible, the date its accuracy was last verified.
  - The title and contact information for the person to whom questions regarding the information, including its accuracy, should be directed. [assessment_07]

Issuance Criteria:
yes(ALL)

Information Sharing Policy: Information Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/PHI-privacy-policy/IS-policy-information/1.0/

Description:
This Trustmark Definition defines requirements for creating the Information aspects of an Information Sharing Policy.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

Information Sharing Policy: Information

Description: The policy MUST contain the required Information sections.

- **Type of Information**: Does the entity's information sharing policy clearly state what information may be sought, retained, shared, disclosed or disseminated, by the entity and whether there are different policy provisions for different types of information (e.g., medical, mental health, and substance abuse information, as well as fact-based information databases)? [assessment_01]
- **Purpose for Use of Information**: Does the entity's information sharing policy clearly state the purpose(s) for which information may be sought, retained, shared, disclosed, or disseminated by the entity? [assessment_02]
- **Disallowed Information**: Does the entity's information sharing policy clearly state what information may not be sought, retained, shared, disclosed, or redisclosed by the entity (e.g., for reasons of discrimination)? [assessment_03]
- **Information Categorization**: Does the entity's information sharing policy clearly state whether the entity categorizes information (or ensures that the PHI-providing entity has categorized information) based on its nature (for example, conditions of supervision, medical, mental health, and substance abuse information), usability, and quality? [assessment_04]
- **Categorization Reevaluation**: Does the entity's information sharing policy clearly state the conditions that prompt the labels cited in 4 above to be reevaluated? [assessment_05]
- **Recording of Source**: Does the entity's information sharing policy clearly state whether the entity maintains a record of the source of the information sought and collected? [assessment_06]

Issuance Criteria:
yes(ALL)

PHI Privacy Policy: Information Quality Assurance Trust Interoperability Profile

URI:
http://ncsc.org/trustmarks/trustmark-definitions/PHI-privacy-policy/PHI-policy-information-quality-assurance-TIP/1.0/

Description:
This Trust Interoperability Profile specifies requirements for creating the Information Quality Assurance of a PHI Privacy Policy for exchanging Protected Health Information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and 42 CFR Part 2.

References

Trustmark Definition Requirements

- PHI Privacy Policy: Information Quality Assurance TD [PHI-G-TD]
- Information Sharing Policy: Information Quality Assurance TD [IS-G-TD]

Trust Interoperability Profiles

- None

Trust Expression:

PHI-G-TD AND IS-G-TD

PHI Privacy Policy: Information Quality Assurance Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/PHI-privacy-policy/PHI-policy-information-quality-assurance/1.0/

Description:
This Trustmark Definition defines requirements for creating the Information Quality Assurance aspects of a PHI Privacy Policy for exchanging Protected Health Information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and 42 CFR Part 2.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

PHI Privacy Policy: Information Quality Assurance

Description: The policy MUST contain the required Information Quality Assurance sections.

- **Procedure for Amending PHI**: Does the entity's PHI privacy policy clearly state, in the case of a HIPAA-covered entity, the entity's procedure for amending PHI if informed by another covered entity of a need to amend an individual's record? [assessment_06]

Issuance Criteria:
yes(ALL)

Information Sharing Policy: Information Quality Assurance Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/PHI-privacy-policy/IS-policy-information-quality-assurance/1.0/

Description:
This Trustmark Definition defines requirements for creating the Information Quality Assurance aspects of an Information Sharing Policy.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

Information Sharing Policy: Information Quality Assurance

Description: The policy MUST contain the required Information Quality Assurance sections.

- **Procedures to Endure Data Quality**: Does the entity's information sharing policy clearly state whether the entity has established procedures and procedures (manual and electronic) to ensure the quality (for example, accurate, complete, current, verifiable, and reliable) of the information it collects, maintains, and disseminates? [assessment_01]
- **Research of Alleged or Suspected Errors**: Does the entity's information sharing policy clearly state whether the entity researches alleged or suspected errors and deficiencies (or refers them to the PHI- providing agency) and how the entity responds to confirmed errors or deficiencies? [assessment_02]
- **Review for Bad Data**: Does the entity's information sharing policy clearly state when the entity reviews the quality of the information it originates and identifies data that may be inaccurate or incomplete, includes incorrectly merged information, is out of date, cannot be verified, has a questionable source, or lacks adequate context such that the rights of the individual may be affected, the entity's procedure for correction or destruction? [assessment_03]
- **Notification to Originating Agency in Case of Bad Data**: Does the entity's information sharing policy clearly state when the entity reviews the quality of the information it has received from an originating agency and identifies data that may be inaccurate or incomplete, includes incorrectly merged information, is out of date, cannot be verified, has a questionable source, or lacks adequate context such that the rights of the individual may be affected, whether the entity notifies the originating agency or the originating agency's privacy officer and the method used to notify the agency (written, telephone, or electronic notification)? [assessment_04]
- **Notification to External Agency in Case of Bad Data**: Does the entity's policy clearly state when the entity reviews the quality of the PHI it has provided to an external agency and identifies data that may be inaccurate or incomplete, includes incorrectly merged information, is out of date, cannot be verified, has a questionable source, or lacks adequate context such that the rights of the individual may be affected, whether the entity notifies the external agency? [assessment_05]

Issuance Criteria:
yes(ALL)

PHI Privacy Policy: Accountability and Enforcement Trust Interoperability Profile

URI:
http://ncsc.org/trustmarks/trustmark-definitions/PHI-privacy-policy/PHI-policy-accountability-and-enforcement-TIP/1.0/

Description:
This Trust Interoperability Profile specifies requirements for creating the Accountability and Enforcement aspects of a PHI Privacy Policy for exchanging Protected Health Information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and 42 CFR Part 2.

References

Trustmark Definition Requirements

- PHI Privacy Policy: Accountability and Enforcement TD [PHI-N-TD]
- Information Sharing Policy: Accountability and Enforcement TD [IS-N-TD]

Trust Interoperability Profiles

- None

Trust Expression:

PHI-N-TD AND IS-N-TD

PHI Privacy Policy: Accountability and Enforcement Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/PHI-privacy-policy/PHI-policy-accountability-and-enforcement/1.0/

Description:
This Trustmark Definition defines requirements for creating the Accountability and Enforcement aspects of a PHI Privacy Policy for exchanging Protected Health Information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and 42 CFR Part 2.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

PHI Privacy Policy: Accountability and Enforcement

Description: The policy MUST contain the required Accountability and Enforcement sections.

- **Information System Transparency: Policy Posted on Web Site**: Does the entity's PHI privacy policy clearly state, if your entity is a HIPAA-covered entity, whether the entity posts its PHI privacy policy on the entity's Web site? [assessment_01-02]
- **Information System Transparency: Requirements Notification to Patients**: Does the entity's PHI privacy policy clearly state, if your entity is a federally assisted program, whether the entity provides a notice to patients of federal confidentiality requirements (e.g., substance abuse information, 42 CFR Part 2)? [assessment_01-03]
- **Information System Transparency: Policy Complaint Process**: Does the entity's PHI privacy policy clearly state whether the entity has a process for individuals to make complaints concerning the entity's policies, procedures, and privacy practices if the individual feels that a violation of HIPAA or 42 CFR Part 2 has occurred? [assessment_01-04]
- **Accountability: Procedures for Evaluation of User Compliance**: Does the entity's PHI privacy policy clearly state the procedures and practices the entity follows to enable evaluation of user compliance with information access requirements, the entity's PHI privacy policy, and applicable law? [assessment_02-03]
- **Accountability: Consent Authorization Retention Periods and Audit Trails Thereof**: Does the entity's PHI privacy policy clearly state the entity's retention period for patient consent authorizations, and whether audits are completed to ensure that appropriate consent authorizations are maintained and current? [assessment_02-05]
- **Enforcement: Authorization Qualifications for Access and Sanctions for Violations**: Does the entity's PHI privacy policy clearly state the entity's policy with regard to the qualifications and number of participating agency personnel authorized to access PHI, and the additional sanctions the entity may utilize for violations of the entity's PHI privacy policy? [assessment_03-02]

Issuance Criteria:
yes(ALL)

Information Sharing Policy: Accountability and Enforcement Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/PHI-privacy-policy/IS-policy-accountability-and-enforcement/1.0/

Description:
This Trustmark Definition defines requirements for creating the Accountability and Enforcement aspects of an Information Sharing Policy.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

Information Sharing Policy: Accountability and Enforcement

Description: The policy MUST contain the required Accountability and Enforcement sections.

- **Information System Transparency: Publicly Available Policy**: Does the entity's information sharing policy clearly state whether the entity's policy is available to the public (for example, provided to the public for review, made available upon request, and/or posted on the entity's Web site—include Web address)? [assessment_01-01]
- **Information System Transparency: Point of Contact for Inquiries and Complaints**: Does the entity's information sharing policy clearly state whether the entity has a point of contact (position/title) for handling inquiries or complaints, and whether the contact information for this individual (for example, phone, Web site, e-mail, or U.S. mail address) is provided? [assessment_01-05]
- **Accountability: User-Identified Access and Logging Thereof**: Does the entity's information sharing policy clearly state whether access (e.g., electronic or hard-copy access) to the entity's data identifies the user, and whether the identity of the user is retained in the audit log? [assessment_02-01]
- **Accountability: Data Log and Audit Trail**: Does the entity's information sharing policy clearly state whether a log (electronic or paper) is kept of accessed and disseminated entity-held data, and whether an audit trail is maintained? [assessment_02-02]
- **Accountability: Mechanism for Reporting Errors and Violations**: Does the entity's information sharing policy clearly state whether the entity has a mechanism for personnel to report errors and suspected or confirmed violations of entity privacy policies related to PHI? [assessment_02-04]
- **Accountability: Auditing Entity**: Does the entity's information sharing policy clearly state whether audits are completed by an independent third party or a designated representative of the entity? [assessment_02-06]
- **Accountability: Review and Update of Policy Provisions**: Does the entity's information sharing policy clearly state how often the entity reviews and updates the provisions contained within the policy (recommendation is annually), and whether a record is kept of all changes to entity information sharing policies, including security provisions and procedures and, if so, the entity's retention period for such documentation? [assessment_02-07]
- **Enforcement: Enforcement Procedures for Noncompliance**: Does the entity's information sharing policy clearly state the procedures for enforcement if entity personnel, a participating agency, or an authorized user is suspected of being or has been found to be in noncompliance with the provisions of the entity's information sharing policy? [assessment_03-01]

Issuance Criteria:
yes(ALL)

Consent Authorizations Profile Trust Interoperability Profile

URI:
http://ncsc.org/trustmarks/trustmark-definitions/consent-authorization/consent-authorizations/1.0/

Description:
This Trust Interoperability Profile defines requirements for HIPAA and 42 CFR Part 2 Compliant Consent Authorizations.

References

Trustmark Definition Requirements

- Consent Authorization Revocation TD [TD_01]

Trust Interoperability Profiles

- Consent Authorization Form Requirements Profile TIP [TIP_01]
- Defective Consent Authorizations TIP [TIP_02]

Trust Expression:

TIP_01 AND TIP_02 AND TD_01

Consent Authorization Revocation Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/consent-authorization/consent-authorization-revocation/1.0/

Description:
This Trustmark Definition defines requirements to determine if a consent authorization has been revoked.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

Authorization Revocation

Description: A consent authorization MUST NOT have been revoked.

- **Revocation by Consenting Individual**: Has the individual revoked the consent authorization? [assessment_01]
- **Action in Reliance of Consent**: Has the covered entity has taken action in reliance the consent authorization? [assessment_02]
- **Insurance Coverage and Contest of Claim** : Was the consent authorization obtained as a condition of obtaining insurance coverage and does other law provides the insurer with the right to contest a claim under the policy or the policy itself? [assessment_03]

Issuance Criteria:
no(assessment_01) OR (yes(assessment_02) OR yes(assessment_03))

Consent Authorization Form Requirements Profile Trust Interoperability Profile

URI:
http://ncsc.org/trustmarks/trustmark-definitions/consent-authorization/consent-authorization-form-requirements/1.0/

Description:
This Trust Interoperability Profile defines requirements for creating HIPAA and 42 CFR Part 2 Compliant Consent Authorization Forms.

References

Trustmark Definition Requirements

- HIPAA Consent Authorization Form Requirements TD [TD_01]
- 42 CFR Part 2 Consent Authorization Form Requirements TD [TD_02]

Trust Interoperability Profiles

- None

Trust Expression:

TD_01 AND TD_02

HIPAA Consent Authorization Form Requirements Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/consent-authorization/HIPAA-consent-authorization-form-requirements/1.0/

Description:
This Trustmark Definition defines requirements for creating a HIPAA Consent Authorization Form.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

HIPAA Consent Authorization Form Requirements - Elements

Description: A consent authorization MUST include the required elements.

- **Information to be Disclosed**: Does the authorization include a description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion? [assessment_01]
- **Identification of Persons Authorized to Request or Disclose**: Does the authorization include the name or other specific identification of the person(s) or class of persons authorized to make the requested use or disclosure? [assessment_02]
- **Identification of Persons Authorized to Receive Disclosure**: Does the authorization include the name or other specific identification of the person(s) or class of persons to whom the covered entity may make the requested use or disclosure? [assessment_03]
- **Purpose of Use or Disclosure**: Does the authorization include a description of each purpose of the requested use or disclosure. Note: The statement “at the request of the individual” is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose? [assessment_04]
- **Expiration Conditions Specified**: Does the authorization include an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. Note: The statement “end of the research study,” “none,” or similar language is sufficient if the authorization is for a use or disclosure of PHI for research, including for the creation and maintenance of a research database or research repository? [assessment_05]
- **Signature of Person Authorizing Disclosure**: Does the authorization include the signature of the individual and date signed. Note: If the authorization is signed by a personal representative of the individual, a description of such representative’s authority to act for the individual also must be provided? [assessment_06]

HIPAA Consent Authorization Form Requirements - Notice Statements

Description: A consent authorization MUST include the required notice statements.

- **Notice of Right to Revoke**: Does the authorization contain statements adequate to place the individual on notice of the individual’s right to revoke the authorization in writing, and either:
  - The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or
  - To the extent that the exceptions to the right to revoke are included in the notice required by HIPAA’s notice of privacy practices for PHI, as per § 164.520, a reference to the covered entity’s notice? [assessment_07]
- **Notice of Ability to Condition on Authorization**: Does the authorization contain statements adequate to place the individual on notice of the ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the authorization, by stating either:
  - The covered entity may not condition treatment, payment, enrollment, or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of

authorizations applies; or
    - The consequences to the individual of a refusal to sign the authorization when the covered entity can, per § 164.508(b)(4), condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization? [assessment_08]
- **Notice of Potential Redisclosure**: Does the authorization contain statements adequate to place the individual on notice of the potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer to be protected? [assessment_09]

Issuance Criteria:
yes(ALL)

42 CFR Part 2 Consent Authorization Form Requirements Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/consent-authorization/24-CFR-part-2-consent-authorization-form-requirements/1.0/

Description:
This Trustmark Definition defines requirements for creating a 42 CFR Part 2 Consent Authorization Form.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

42 CFR Part 2 Consent Authorization Form Requirements - Elements

Description: A consent authorization MUST include the required elements.

- **Identification of Entity Making the Disclosure**: Does the written consent to a disclosure include the specific name or general designation of the program or person permitted to make the disclosure? [assessment_01]
- **Identification of Entity Receiving the Disclosure**: Does the written consent to a disclosure include the name or title of the individual or the name of the organization to which disclosure is to be made. Note: The authorization has to specifically state the name of the provider or the general designation of the treatment center (e.g., Shady Grove Substance Abuse Center)? [assessment_02]
- **Patient Name**: Does the written consent to a disclosure include the name of the patient? [assessment_03]
- **Purpose of Disclosure**: Does the written consent to a disclosure include the purpose of the disclosure? [assessment_04]
- **Kind and Amount to be Disclosed**: Does the written consent to a disclosure include how much and what kind of information is to be disclosed? [assessment_05]
- **Signature of Authorizing Person**: Does the written consent to a disclosure include the signature of the patient and, when required for a patient who is a minor, the signature of a person authorized to give consent under § 2.14; or, when required for a patient who is incompetent or deceased, the signature of a person authorized to sign under § 2.15 in lieu of the patient? [assessment_06]
- **Date Consent Form Signed**: Does the written consent to a disclosure include the date on which the consent is signed? [assessment_07]
- **Expiration Conditions Specified**: Does the written consent to a disclosure include the date, event, or condition upon which the consent will expire if not revoked before. This date, event, or condition must ensure that the consent will last no longer than reasonably necessary to serve the purpose for which it is given? [assessment_08]

42 CFR Part 2 Consent Authorization Form Requirements - Notice Statements

Description: A consent authorization MUST include the required notice statements.

- **Notice of Potential Revocation**: Does the authorization contain statements adequate to place the individual on notice that the consent is subject to revocation at any time, except to the extent that the program or person making the disclosure has already acted in reliance on it. Acting in reliance includes the provision of treatment services in reliance on a valid consent to disclose information to a third-party payer? [assessment_09]
- **Notice of Subsequent Redisclosure**: Under 42 CFR Part 2, a single consent form can authorize a disclosure of information about a patient to one recipient, and simultaneously authorize that recipient to redisclose that information to any additional entity or entities (such as other affiliated health-care providers identified in the consent form), provided that the purpose for the disclosure is the same. Does the authorization contain the following required statement prohibiting redisclosure,

so that each subsequent recipient of that information is notified of the prohibitions on redisclosure?

This notice covers the disclosure of information to you concerning a client in alcohol/drug treatment, made to you with the consent of such client. This information has been disclosed to you from records protected by federal confidentiality rules (42 C.F.R. Part 2). The federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 C.F.R. Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The federal rules restrict any use of the information to criminally investigate or prosecute any substance abuse patient. [assessment_10]

Issuance Criteria:
yes(ALL)

Defective Consent Authorizations Profile Trust Interoperability Profile

URI:
http://ncsc.org/trustmarks/trustmark-definitions/consent-authorization/defective-consent-authorizations/1.0/

Description:
This Trust Interoperability Profile specifies requirements for creating a generic Policy.

References

Trustmark Definition Requirements

- HIPAA Defective Consent Authorizations TD [TD_01]
- 42 CFR Part 2 Defective Consent Authorizations TD [TD_02]

Trust Interoperability Profiles

- None

Trust Expression:

TD_01 AND TD_02

HIPAA Defective Consent Authorizations Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/consent-authorization/HIPAA-defective-consent-authorizations/1.0/

Description:
This Trustmark Definition defines requirements to determine if a consent authorization is not defective.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

HIPPA Defective Authorizations

Description: A consent authorization MUST NOT be defective.

- **Expiration**: Has the expiration date passed or does the covered entity know that the expiration event has occurred? [assessment_01]
- **Completeness**: Has the authorization been filled out completely, with respect to required elements? [assessment_02]
- **Revocation**: Does covered entity know that the authorization has been revoked? [assessment_03]
- **False Information**: Is any material information in the authorization known by the covered entity to be false? [assessment_04]

Compound Authorizations

Description: A compound consent authorization MUST NOT be defective.

- **Compound Authorizations**: Is the authorization combined with any other document to create a compound authorization? [assessment_05]
- **Research Studies**: Is the authorization for a research study and is combined with any other type of written permission for the same research study, including another authorization for the use or disclosure of PHI for such research or a consent to participate in such research? [assessment_06]
- **Psychotherapy Notes**: Is the authorization for a use or disclosure of psychotherapy notes and is combined only with another authorization for a use or disclosure of psychotherapy notes? [assessment_07]
- **Psychotherapy Notes**: Is the authorization for a use or disclosure of psychotherapy notes and is combined with any other such authorization under this Trustmark Definition? [assessment_08]

Prohibition on Conditioning of Authorizations

Description: A consent authorization MUST NOT violate requirements involving authorizations being used as a condition for other services.

- **Conditioned Authorizations**: Does the covered entity condition the provision treatment, payment, enrollment in a health plan, or eligibility for benefits to an individual on a Consent Authorization? [assessment_09]
- **Research-Related Treatment**: Is a covered health-care provider conditioning the provision of research-related treatment on a consent authorization for the use or disclosure of PHI for such research? [assessment_10]
- **Health Care Plan Enrollment and Benefits**: Is a covered health-care provider conditioning health plan enrollment or eligibility for benefits on a consent authorization requested by the health plan *prior* to an individual's enrollment in the health plan, and the authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk-rating determinations, and the authorization is not for a use or disclosure of psychotherapy notes?

[assessment_11]

- **PHI-Creation-Specific Health Care**: Is the health care being provisioned solely for the purpose of creating PHI for disclosure to a third party on provision of an authorization for the disclosure of the PHI to such third party? [assessment_12]

Issuance Criteria:
(no(assessment_01) AND yes(assessment_02) AND no(assessment_03) AND no(assessment_04)) AND (!yes(assessment_05) OR yes(assessment_06) OR yes(assessment_07)) AND (!yes(assessment_09) OR yes(assessment_10 OR yes(assessment_11) OR yes(assessment_12))

42 CFR Part 2 Defective Consent Authorizations Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/consent-authorization/42-CFR-part-2-defective-consent-authorizations/1.0/

Description:
This Trustmark Definition defines requirements to determine if a consent authorization is not defective.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

HIPAA Consent Authorization Form Requirements - Elements

Description: A consent authorization MUST include the required elements.

- **Expiration**: Has the consent form expired? [assessment_01]
- **Revocation**: Is the consent form known to have been revoked? [assessment_02]
- **Material Falsehood**: Is the consent form known, or through a reasonable effort could be known, by the person holding the records to be materially false? [assessment_03]

Issuance Criteria:
no(ALL)

Contractual Agreements Profile Trust Interoperability Profile

URI:
http://ncsc.org/trustmarks/trustmark-definitions/contractual-agreements/contractual-agreements-TIP/1.0/

Description:
This Trust Interoperability Profile specifies requirements for Contractual Agreements between HIPAA-Covered Entities and Business Associates/Qualified Service Organizations.

References

Trustmark Definition Requirements

- HIPAA Business Associate TD [TD_01]
- Business Associate/Qualified Service Organization Agreements TD [TD_02]
- Redress Policy TD [TD_03]

Trust Interoperability Profiles

- None

Trust Expression:

TD_01 AND TD_02 AND TD_03

HIPAA Business Associate Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/contractual-agreements/HIPAA-Business-Associate/1.0/

Description:
This Trustmark Definition defines conformance and assessment criteria for compliance with minimum security requirements for acceptance criteria as related to overall system and services acquisition requirements.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

Valid HIPAA Business Associate

Description: The organization MUST be a valid HIPAA Business Associate.

- **Not a HIPAA Covered Entity**: Is the organization a HIPAA covered Entity? [assessment_01]
- **Provides Covered Functions or Activities**: Does the organization perform any of the following functions or activities that involve the use or disclosure of PHI on behalf of a covered entity? (Claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, or repricing.) [assessment_02]
- **Provides Covered Services**: Does the organization provide any of the following services that involve the use or disclosure of PHI to a covered entity? (Legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial.) [assessment_03]

Issuance Criteria:
no(assessment_01) and (yes(assessment_02) or yes(assessment_03))

Business Associate/Qualified Service Organization Agreements Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/contractual-agreements/Business-Associate-Agreements/1.0/

Description:
This Trustmark Definition defines requirements for a HIPAA Business Associate's contractual agreements with HIPAA-covered entities.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

Contractual Agreements with HIPPA-Covered Entities

Description: The organization's contractual agreements with HIPAA-covered entities MUST meet requirements.

- **Agreement to Limit Disclosure**: Do the organization's contracts contain language concerning the Business Associate agreeing to not use or disclose PHI other than as permitted or required by the Agreement or as Required by Law? [assessment_01]
- **Safeguards to Limit Disclosure**: Do the organization's contracts contain language concerning the Business Associate agreeing to use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by the Agreement? [assessment_02]
- **Agreement to Comply with Requirements**: Do the organization's contracts contain language concerning the Business Associate agreeing to comply with applicable security, administrative, physical, and technical safeguards requirements at both the State and Federal levels? [assessment_03]
- **Data Breach Notification**: Do the organization's contracts contain language concerning notification of HIPAA-Covered Entity in case of data breach? [assessment_04]
- **Data Breach Damage Mitigation**: Do the organization's contracts contain language concerning mitigating damages in case of data breach? [assessment_05]
- **Outside Use Notification**: Do the organization's contracts contain language concerning notification to HIPAA-Covered Entity of uses outside the scope of the agreement? [assessment_06]
- **Limits on Passing Data**: Do the organization's contracts contain language limiting the passing on of data only with the same agreement bound to agents or sub-contractors? [assessment_07]
- **Data Availability on Entity Direction**: Do the organization's contracts contain language concerning agreements to make data available on direction of HIPAA-Covered Entity? [assessment_08]
- **Data Update on Entity Direction**: Do the organization's contracts contain language concerning agreements to update data on direction of HIPAA-Covered Entity? [assessment_09]
- **Assessements Policy**: Do the organization's contracts contain language concerning the availability of policies, etc, to HHS to allow for assessments? [assessment_10]
- **Documentation of Disclosures**: Do the organization's contracts contain language concerning documenting disclosures for purpose of accounting of those disclosures? [assessment_11]
- **Providing of Documentation of Disclosures**: Do the organization's contracts contain language concerning providing documentations of disclosures for the purpose of accounting of those disclosures? [assessment_12]
- **Allowed Purposes**: Do the organization's contracts contain language specifying purposes for which PHI may be disclosed or alternately refer to a services agreement providing such information? [assessment_13]
- **Use and Disclosure Provisions**: Do the organization's contracts contain language concerning specific use and disclosure provisions? [assessment_14]
- **Communication of Privacy Practices and Restrictions**: Do the organization's contracts contain language concerning provisions for HIPAA-Covered Entity to inform Business Associate of privacy practices and restrictions, dependent on specific business arrangements? [assessment_15]
- **Permissible Entity Requests**: Do the organization's contracts contain language concerning

descriptions of permissible requests by HIPAA-Covered Entity? [assessment_16]

- **Term of Agreement**: Do the organization's contracts contain language concerning the term of the agreement, including effective date and date or conditions of termination? [assessment_17]
- **Termination Procedures**: Do the organization's contracts contain language concerning termination procedures when termination for cause occurs? [assessment_18]
- **Post-Termination Procedures**: Do the organization's contracts contain language concerning post-termination procedures, including subsequent destruction of PHI? [assessment_19]

Issuance Criteria:
yes(ALL)

Redress Policy Trustmark Definition

URI:
http://ncsc.org/trustmarks/trustmark-definitions/contractual-agreements/Redress-Policy/1.0/

Description:
This Trustmark Definition defines conformance for an organization having a Redress Policy.

Metadata

Key	Value
tf:TargetStakeholderDescription	Organizations that are interested in safely and legally exchanging information in a manner that complies with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRecipientDescription	Organizations that want to demonstrate that they provide and/or consume digital information services in a manner that complies with with HIPAA and 42 CFR Part 2 regulations.
tf:TargetRelyingPartyDescription	Organizations and individuals that require their trusted partners' computer and information systems to comply with HIPAA and 42 CFR Part 2 regulations.
tf:TargetProviderDescription	Organizations that audit or evaluate other organizations for compliance with HIPAA and 42 CFR Part 2 regulations.
tf:ProviderEligibilityCriteria	Any organization or business entity may act as a Trustmark Provider for trustmarks under this Trustmark Definition.
tf:AssessorQualificationsDescription	Any individual employed or contracted by the Trustmark Provider may act as the assessor for trustmarks under this Trustmark Definition.
tf:TrustmarkRevocationCriteria	For any trustmark issued under this Trustmark Definition, the Trustmark Provider must revoke the trustmark upon any condition whereby one or more Conformance Criteria cease to be satisfied.
tf:ExtensionDescription	This Trustmark Definition requires no extension data.
tf:LegalNotice	This document and the information contained herein is provided on an “AS IS” basis, and the National Center for State Courts disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties or merchantability or fitness for a particular purpose. In addition, the National Center for State Courts disclaims legal liability for any loss incurred as a result of the use or reliance on the document or the information contained herein.
tf:Notes	The National Center for State Courts (NCSC) has published this document with the support of the [TBD] via [TBD]. The views expressed herein do not necessarily reflect the official policies of NCSC, [TBD], or [TBD]; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Conformance Criteria

Redress Policy

Description: The organization MUST have an acceptable Redress Policy.

- **Disclosure Notice**: Does the organization's Redress Policy disclose to individual about whom the information was gathered the conditions under which the entity will disclose PHI information? [assessment_01]
- **Disclosure Record**: Does the organization keep a record of all requests and of what information is disclosed to an individual? [assessment_02]
- **Disclosure Exceptions**: Does the organization document exceptions when the individual about whom the information was gathered is not notified? This includes whether the entity refers the individual to the agency originating the information? [assessment_03]
- **Data Amendments**: Does the organization perform any of the following functions or activities that involve the use or disclosure of PHI on behalf of a covered entity? (Claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, or repricing.) [assessment_04]
- **Data Amendment Point of Contact**: Does the organization provide any of the following services that involve the use or disclosure of PHI to a covered entity? (Legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial.) [assessment_05]
- **Data Amendment Retention Record**: Does the organization provide any of the following services that involve the use or disclosure of PHI to a covered entity? (Legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial.) [assessment_06]
- **Data Amendment Point of Contact**: Does the organization provide a point of contact for handling individuals' requests for amendments of PHI? [assessment_07]
- **Data Amendment Procedure**: Does the organization have a procedure for handling individuals' requests for correction (or amendments) involving information that the entity can change because it originated the information? [assessment_08]
- **Data Amendment Record**: Does the organization maintain a record of requests for corrections (amendments) [assessment_09]
- **Appeal Conditions**: Does the organization document the conditions under which the entity may deny an individual's request for access or correction (amendment)? [assessment_10]
- **Appeal Procedure**: If requests for access or corrections (amendments) are denied, does the entity have a procedure for appeal (or review)? [assessment_11]

Issuance Criteria:
yes(ALL)

Glossary

Term	Definition
Authorization	The process of granting a person, computer process, or device with access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access that is verified through authentication.
Disclosure	The release, transfer, provision of access to, sharing, publication, or divulging of personal information in any manner—electronic, verbal, or in writing—to an individual, entity, or organization outside the entity that collected it. Disclosure is an aspect of privacy focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.
HIPAA	Health Insurance Portability and Accountability Act of 1996
PHI	Protected Health Information
Redress	Laws, policies, and procedures that address public entity responsibilities with regard to access/disclosure and correction of information and the handling of complaints from persons regarding protected information about them which is under the entity's control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.