Contractual Agreements Profile Trust Interoperability Profile

Table of Contents

Overall Organization

- Contractual Agreements Profile TIP
  - HIPAA Business Associate TD
  - Business Associate/Qualified Service Organization Agreements TD
  - Redress Policy TD

Trustmark Definition Checklist

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)

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
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.