DirectTrust®
Accreditation
Governed by EHNAC

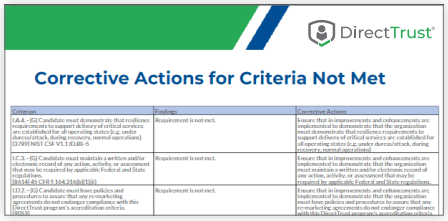


DirectTrust Accreditation Reports: Supporting Continuous Improvement and Compliance

Demonstrating privacy and security compliance against industry standards is more critical than ever. Upon achieving full accreditation, we provide organizations with a suite of comprehensive reports for both internal and external stakeholders, communicating compliance status, addressing gaps, and supporting future improvements.

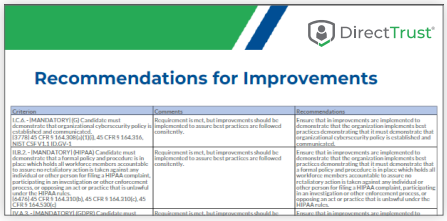
Executive Summary Report

Designed for senior leadership, this concise overview highlights key findings, compliance status, and an organization's overall accreditation assessment. The final sections, "Corrective Actions for Criteria Not Met" and "Recommendations for Improvements," ensure that organizations receive targeted guidance for strengthening their compliance posture.


DirectTrust

Corrective Actions for Criteria Not Met

Criterion	Findings	Corrective Actions
1.A.4. - (G) Candidate must demonstrate that resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations) (3.7.1(b)) NIST CSF V1.1 ID.BE-5	Requirement is not met.	Ensure: that in improvements and enhancements are implemented to demonstrate that the organization must demonstrate that resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations)
1.C.3. - (G) Candidate must maintain a written and/or electronic record of any action, activity, or assessment that may be required by applicable Federal and State statutes. (164.316(b)(1)(ii))	Requirement is not met.	Ensure: that in improvements and enhancements are implemented to demonstrate that the organization must maintain a written and/or electronic record of any action, activity, or assessment that may be required by applicable Federal and State statutes.
1.D.2. - (G) Candidate must have policies and procedures to assure that any re-marketing agreements do not endanger compliance with this DirectTrust program's accreditation criteria. (1.B.6.3)	Requirement is not met.	Ensure: that in improvements and enhancements are implemented to demonstrate that the organization must have policies and procedures to assure that any re-marketing agreements do not endanger compliance with this DirectTrust program's accreditation criteria.


DirectTrust

Recommendations for Improvements

Criterion	Comments	Recommendations
1.C.A. - (MANDATORY) (G) Candidate must demonstrate that organizational cybersecurity policy is established and communicated. (3.7.1(b) 45 CFR § 164.308(a)(1)(i), 45 CFR § 164.316, NIST CSF V1.1 ID.GV-1	Requirement is met, but improvements should be implemented to assure best practices are followed consistently.	Ensure: that in improvements are implemented to demonstrate that the organization implements best practices demonstrating that it must demonstrate that organizational cybersecurity policy is established and communicated.
II.B.2. - (MANDATORY) (HIPAA) Candidate must demonstrate that a formal policy and procedure is in place which holds all workforce members accountable for assure no retaliatory actions is taken against any individual or other person for filing a HIPAA complaint, participating in an investigation or other enforcement process, or opposing an act or practice that is unlawful under the HIPAA rules. (§§ 160.316 45 CFR § 164.530(g), 45 CFR § 164.310(c), 45 CFR § 164.530(e))	Requirement is met, but improvements should be implemented to assure best practices are followed consistently.	Ensure: that in improvements are implemented to demonstrate that the; organization implements best practices demonstrating that it must demonstrate that a formal policy and procedure is in place; which holds all workforce members accountable for assure no retaliatory actions is taken against; any individual or other person for filing a HIPAA complaint, participating in; an investigation or other enforcement process, or opposing; an act or practice that is unlawful under the HIPAA rules.
IV.A.3. - (MANDATORY) (GDPR) Candidate must	Requirement is met, but improvements should be	Ensure: that in improvements are implemented to

Full Report

A deep dive into the accreditation process, the Full Report is significantly longer than the Executive Summary, providing detailed insights that may also satisfy third-party security assessment requirements. The report's DirectTrust Assessment section provides a comprehensive evaluation of all detailed criteria and responses, methodically reviewing compliance with industry standards. The Full Report also concludes with "Corrective Actions for Criteria Not Met" and "Recommendations for Improvements," reinforcing our commitment to continuous improvement by outlining areas in need of enhancement and best practice recommendations.


DirectTrust

DirectTrust Assessment

Organization: Fictitious, Inc.
DirectTrust Program and Version: Health App V1.0
DirectTrust Primary Reviewer: Ralph Zurn

Mandatory Met: YES
Accreditation Status: Full
- Full Accreditation: 85% - 100%
- Provisional Accreditation: 75% - 84%
- Denied Accreditation: < 75%

Summary Report for Third Parties

Tailored for external stakeholders, this summary confirms accreditation status without disclosing sensitive details. Organizations can use this report to demonstrate compliance to partners and clients who require proof of accreditation without extensive documentation.

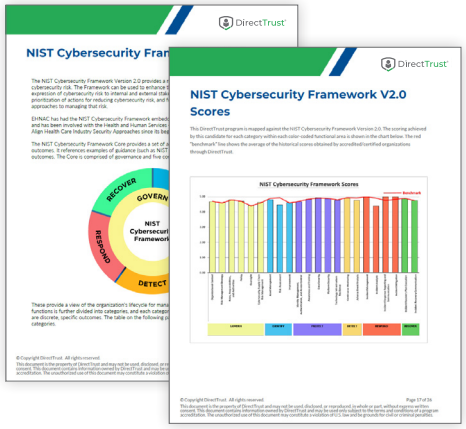


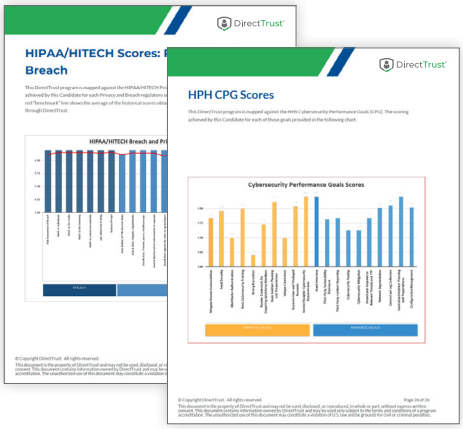
DirectTrust®
Accreditation
Governed by EHNAC

Recognized Security Practices (HIPAA Safe Harbor) Reports

Our accreditation programs align with the 2021 HIPAA Safe Harbor Law (H.R. 7898 – Public Law 116-321) which offers reduced enforcement penalties and audit scrutiny for organizations. This demonstrates compliance with Recognized Security Practices (RSP) for at least 12 months including alignment with:

- HIPAA Security and Privacy Rules
- The NIST Cybersecurity Framework
- HITECH Breach Act requirements
- NIST SP 800-171 Rev2 security controls





HHS Cybersecurity Performance Goals (CPGs)

The RSP Report also includes evaluations against HHS Cybersecurity Performance Goals, a voluntary framework that enhances cyber preparedness, resilience, and protection of patient data. These goals are informed by industry-recognized frameworks, such as NIST 800-53 Revision 5, ensuring alignment with industry best practices. Graphical compliance scoring within the report provides an at-a-glance view of adherence to security and privacy standards, helping organizations easily track progress.

Note: RSP Reports are not generated for TNAP, TDRAAP, and EPCS programs due to program scope. Additionally, if a HITRUST Validated Report is used to fulfill Security controls, an RSP report will not be issued, as HITRUST provides equivalent documentation.

Additional Reporting and Support

DirectTrust understands the importance of demonstrating trust in healthcare data management. Upon request, additional reports—including program-to-program crosswalks—can be provided. For more information or to request additional reports, contact the DirectTrust Operations team.

DirectTrust® is a non-profit, vendor-neutral alliance dedicated to establishing trust in a connected world. The organization serves as a forum for a consensus-driven community focused on health communication and cybersecurity, an ANSI standards development organization, an accreditation and certification body governed by EHNAC, and a developer of trust frameworks and supportive services for secure information exchange like Direct Secure Messaging and identity-verified credentials.

Admin@DirectTrust.org
DirectTrust.org