



DirectTrust Assessment with Accreditation Summary Report for Third Parties

Updox

Commission Approval Date: 07/09/2024

Governed by the Electronic Healthcare Network Accreditation Commission (EHNAC)

For additional information see the DirectTrust website at www.DirectTrust.org

DirectTrust Overview

History

The Electronic Healthcare Network Accreditation Commission (EHNAC) is the governing body of DirectTrust. In 2023, EHNAC merged with DirectTrust. EHNAC was founded in 1993 as an independent, federally recognized, standards development organization and tax-exempt, 501(c)(6) non-profit accrediting body designed to improve transactional quality, operational efficiency, and data security in healthcare.

EHNAC grew out of the 1993 Workgroup for Electronic Data Interchange (WEDI), sponsored by the Network Architecture and Accreditation Technical Advisory Group. The healthcare transactions industry agreed there was a need for a self-governing body to develop standards for the industry, and the Association for Electronic Health Care Transactions (AFEHCT) championed the cause by sponsoring an Accreditation Workgroup. Funded by a loan from AFEHCT, EHNAC was born and began accrediting electronic health networks in 1995.

Advancing healthcare through standards

An independent, self-governing body, DirectTrust represents a diverse cross-section of healthcare stakeholders including electronic health networks, payers, hospitals, physicians, consumer groups, financial services firms, state regulators, security organizations, and vendors. DirectTrust's publicly available accreditation criteria are developed and continually enhanced through the input of these industry experts who all work together to establish sound criteria for third-party review and accreditation.

DirectTrust's accreditation programs are governed by the Commission (EHNAC), guided by peer evaluation, and confer upon their recipients a nationally recognized healthcare accreditation. The programs are based on annual risk assessments and are supported through ongoing risk management processes across people, processes, and technology. Accreditation programs include a common set of cyber health security baseline criteria and are augmented by stakeholder sector-specific criteria addressing the requirements unique to that sector.

Most programs include criteria that address HIPAA privacy, security, and breach reporting requirements including updates from HITECH and the Omnibus Rule. Additional requirements are included in each EHNAC program addressing NIST SP 800-53 Security Control areas.

Accreditation encompasses a rigorous organizational self-assessment followed by a site review/audit to evaluate evidentiary compliance.

Intended Use

This report, including all comments, the descriptions of tests, and the determination of compliance against the criteria, is provided solely for the information and use of the organization reviewed by DirectTrust and any other entity with which it chooses to share the report. Entities with whom this report is shared must understand:

- the nature of the services provided by the organization;
- how the organization's system interacts with its users, subcontractors, business associates, and other parties;
- internal control and its limitations;
- the content and scope of this program; and
- the risks that may threaten the achievement of the criteria, and how controls address those risks.

This report is not intended to be and should not be used by anyone other than these specified parties.

In addition to this report, organizations achieving Full Accreditation receive a digital credential that does not contain confidential information and is thus suited for public distribution.

Table of Contents

DirectTrust Overview	2
Intended Use	3
DirectTrust Program in Scope	5
Organization's Responsibilities	6
DirectTrust's Responsibilities	7
Inherent Limitations	8
Opinion	9
Description of Environment and Scope of Review	10
Description of Tests of Controls	12
Management's Acceptance	13
DirectTrust Assessment	14

DirectTrust Program in Scope

EHNAC Program in Scope: DT P&S with HITRUST

The DT P&S program is for health information “trusted agent” service providers (such as an EHR service provider) that act as a Health Information Service Provider (HISP), a Certification Authority (CA), and/or a Registration Authority (RA).

This program accredits against HIPAA Privacy and Security requirements for organizations also pursuing DirectTrust accreditation as a HIS, a Certificate Authority (CA), and/or Registration Authority (RA).

Organization's Responsibilities

Organizations must choose the program for which they seek accreditation. Information on all programs is available on the DirectTrust website (www.DirectTrust.org). Both first-time applicants and re-accrediting organizations follow the same process for achieving accreditation. The accreditation cycle is 2 years. An optional Midterm accreditation is also available for demonstrating to third parties the organization's ongoing security and privacy posture between the full accreditation cycles.

Organizations must review the guidelines which include:

- completing the application process, and signing an Application Agreement and Sentinel Events form;
- submitting a revenue verification form; and
- arranging for payment of application fees.

Once an organization is approved by the Commission, it is given eight months to complete its self-assessment. Organizations are required to provide a written response to each applicable criterion within the self-assessment and to provide evidence in the form of policies, procedures, and samples of implemented controls. Self-assessments are due to be submitted four months prior to the organization's expiration date.

Organizations are then responsible for hosting on-site (or in some cases, remote) visits to each in-scope site, which are arranged by the DirectTrust Assessor. Organizations will respond to outstanding questions during the site visits and support physical tours of the in-scope facilities.

For organizations electing to undergo Midterm reviews, organizations will be required every other year to complete a self-assessment against a set of criteria that covers Privacy, Breach, and Security. Standard criteria are included addressing risk, privacy, breach, and training, plus randomly selected criteria with at least one criterion from each of the security sections. Progress against recommendations found in the previous review must also be reported.

DirectTrust's Responsibilities

In accordance with the Electronic Healthcare Network Accreditation Commission charter and self-governing body, this formally recognized Standards Development Organization conducts its operations via the following principles:

- Pricing, process information, materials, and organization status are made available via the organization's website so that this information is provided transparently and is always made readily accessible.
- DirectTrust staff is thoroughly vetted and background and reference checks are conducted to assure that each Assessor possesses appropriate credentials, years of healthcare-related experience, and subject matter expertise in the areas of privacy, security, interoperable data exchange, and compliance.
- Conduct and written and verbal communications are provided under the direction and guidance and in accordance with the Commissioners and respective committees (such as the Criteria Council).
- Assessment work is conducted as consistently as possible across all organizations regardless of the individual Assessors.
- Materials are prepared with the utmost professionalism, and quality reviews are conducted prior to release to organizations and finalization by the Commissioners.

Inherent Limitations

While DirectTrust's programs report against industry-established privacy, security, and stakeholder-specific criteria, the assessment reports are designed for a broad range of users. Consequently, these might not in some cases include every aspect of the systems and services that its users consider important to their own particular needs.

Evaluations provided are based on the time at which they were made. The projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the criteria is subject to the risk that the system may change or that controls at an organization or its subcontractors or service providers may become inadequate or fail.

The information gathered is subject to inherent limitations and, accordingly, control failures could occur and not be detected.

Opinion

In our opinion, developed from guidelines provided by DirectTrust's governing bodies and healthcare industry subject matter expertise and based on the completed self-assessment criteria responses, corresponding evidence, and site interviews and evaluations:

- a. The self-assessment materials and this resulting report fairly present the organization's operation and system(s) designed and implemented as of the date the materials were formally submitted and are valid throughout the two-year accreditation cycle as represented on the ehnac.org public website.
- b. The evidence provided, both in written form in response to the criteria and via interviews and selected testing, was found to be suitably designed to provide reasonable assurance that the organization's privacy and security would be met if the controls will be effective throughout the two-year accreditation period (with the exception of a Sentinel Event being issued).

Description of Environment and Scope of Review

Name of organization: Updox LLC

Company overview:

Updox cares about our customers, their users, and the safety of the PHI/PII that is entrusted to us therefore Updox has chosen to remain accredited in areas such as privacy and security. We have chosen leaders in the field to perform independent audits of our policies, procedures, technical, operations, and many other areas to ensure current and potential customers understand how important we believe their business and their data is. DirectTrust and EHNAC are leaders in their industry and bring in auditors to assess Updox every two years.

Updox has implemented HIPAA privacy, security, and other policies and procedures required to securely store and transmit protected health information (PHI). As a regulatory requirement and a best practice for business, Updox maintains HIPAA Business Associate Agreements which are contained within the Evercommerce Master Services Agreement and are in place with EHR vendor partners, customers, and sub-contractors.

Updox:

- uses highly respected 3rd party data centers for the storage and processing of all sensitive data, including PHI.
- conducts regular internal and external reviews to assess security and risk of its infrastructure and data.
- has three other accreditations, in addition to the EHNAC/DT Privacy & Security Accreditation and is also certified with the 2015 ONC Health IT criteria for security and HISP operations.
- employees attend training throughout the year pertinent to their responsibilities including HIPAA Privacy and Security training. EverCommerce has ongoing monthly training and additional training as needed to ensure employee knowledge is current with regulations.
- has a dedicated Security and DevOps team responsible for the network, security, and authentication processes.
- has dedicated support teams to assist customers and partners with their questions and issues.
- uses a robust agile development life cycle to ensure quality and effectiveness of its products.

Through evidence presented and performance within the health IT community Updox has a proven record of outstanding reviews and satisfaction with its current partners and customers. As progress and needs constantly evolve in this field Updox is dedicated to providing the best products, exceptional customer service, and leading technology, all while maintaining security for all. Updox continues to strive to meet and exceed expectations from regulatory authorities, current customers/partners and for prospects.

EHNAC program:

Updox is seeking accreditation on the DT P & S w/ HITRUST

Scope of services reviewed including location(s) and system(s):

6555 Longshore St., Dublin, Ohio 43017

- Identification of data flows of confidential information such as Protected Health Information within the organization as well as with business partners outside of the organization;
- Verification that appropriate Business Associate Agreements are in place with all relevant entities;
- Review of HIPAA privacy policies and procedures;
- Review of HIPAA security safeguards in place (administrative, technical and physical);
- Review methods of secure transmission of data;
- Review of customer service metrics;
- Validation of accuracy of transaction exchange;
- Validation of system availability and capacity metrics;
- Validation of compliance with industry standards;
- Review of IT security best practices;
- Review of industry-specific best practices;
- Review of disaster recovery and business continuity processes;
- Review of workforce training; and
- Review of personnel qualifications.

Description of services reviewed:

- **transaction accountability and performance;**
- **key customer satisfaction metrics maintained;**
- **conducting business in a fair and honest manner;**
- **providing a workforce that is trained and resilient;**
- **facilities and systems that are properly managed with capacity assurance;**
- **maintenance of facilities and systems with resiliency and disaster preparedness; and**
- **scrutinizing third parties through interviews and on-site visits.**

Description of Tests of Controls

The specific criteria and associated requirements that were tested, along with a determination of compliance against those criteria, are provided in the DirectTrust Review section.

DirectTrust's standard testing methodology includes the following:

- a careful review of the flow of PHI into and out of the specific services under review
- for programs containing HIPAA Privacy criteria:
 - the evaluation of a DirectTrust-supplied PHI Level Survey wherein assessment is conducted against the organization to ascertain its degree of responsibility against the HIPAA Privacy Rule; and
 - a review of the full organization with respect to HIPAA policies and procedures, including breach reporting, training, flow of PHI between the organization and third parties, and protection of PHI
- on-site (or in some cases, remote) visits with the organization under review as well as all third parties with which the organization shares PHI. This includes visits to data centers, customer support centers, printing operations, managed services organizations, etc. In-scope sites are determined based on the DirectTrust Location Review Policy

The stated purposes of DirectTrust's location reviews are:

1. Organization Interviews

DirectTrust Assessors are expected to interview key personnel including subject matter experts regarding representations made in the self-assessment. The interviews are instrumental in obtaining an understanding of the organization and in understanding how specific services under review are delivered.

2. Verification of Representations

The location review will include random testing to ensure that what is represented in the self-assessment is indeed verifiable. This could include, for example, testing employee knowledge for training received, walkthrough of physical resources described, evaluation of disaster recovery testing, inspection of system and network configurations, etc.

3. Consultative Value to Organization

A key component of each review is the value the DirectTrust Assessor provides to the organization. Each Assessor brings a wealth of industry experience that provides valuable insight to the organization under review.

*This does not apply to certain programs, such as those that certify specific software applications only.

Management Acceptance

Date of Acceptance: 6/17/2024

Organization Name: **updox LLC/ Compliance**

Product Name and Version (Only if this is an Application assessment, such for EPCSCP, Health App, UDAP, or PMSAP accreditation):

With respect to this Report and the related self-assessment, interviews, site visits, and follow-up materials provided, we confirm to the best of our knowledge that:

1. The Description of Environment and Scope of Review section of this report is accurate;
2. Representations made and DirectTrust's assessment of these representations are correct and complete as of the date of this report;
3. Management has reviewed the report and we attest that it properly represents our compliance against the stated controls for the services reviewed under this program;
4. We have properly disclosed any deficiencies and such are appropriately noted in our report;
5. Management recognizes its responsibility to assure the proper implementation of these controls for the periods reviewed and in an ongoing manner; and
6. Management has signed the Sentinel Events Agreement, demonstrating that if any changes to the control areas occur as defined in that agreement we will report such occurrence within the timeframes required within that agreement.

Management accepts this report and will appropriately address each recommendation provided through our formal Risk Management process and by the next accreditation cycle.

Signed,



6/17/2024

Title: **Kallin Brooks**
Director, Compliance. EverHealth, Updox

DirectTrust Assessment

Organization: Updax

DirectTrust Program and Version: DT P&S with HITRUST V2.2

This report includes certain Privacy and Security criteria and requirements from HITRUST CSF© Version V9.6.2. HITRUST CSF© and all associated content is the property of HITRUST Alliance, Inc.

DirectTrust Primary Reviewer: Mark McLaughlin

Mandatory Met: YES

Accreditation Status: Full

- Full Accreditation: 85% - 100%
- Provisional Accreditation: 75% - 84%
- Denied Accreditation: < 75%