Business Risk Planning

SENTINEL EVENTS

DirectTrust Background

DirectTrust™ is a non-profit, vendor-neutral alliance initially created by and for participants in the healthcare and technology communities, including Health Information Service Providers (HISPs), Certificate Authorities (CAs), Registration Authorities (RAs), healthcare providers, pharmaceutical companies, consumers/patients, and health IT vendors. DirectTrust serves as a governance forum, trust community, standards organization, and accreditation body for persons and entities engaged in exchange utilizing PKI mechanisms for trusted, secure information exchange like Direct Secure Messaging and trusted, compliant document submission. The goal of DirectTrust is to develop, promote, and, as necessary, help enforce the rules and best practices necessary to maintain security and trust within its trust community. DirectTrust is committed to fostering widespread public confidence in the interoperable exchange of health information. To learn more, visit www.directtrust.org.

DirectTrust Mission Statement

The Mission of DirectTrust is to support health information exchange that is secure, interoperable, affordable, ubiquitous and usable by diverse end-users. The Mission is pursued in the interest of the public good, as a non-profit, competitively neutral, membership 'learning organization' for voluntary self- governance of health information exchange.

Business risk evaluation is necessary for DirectTrust to accomplish the following objectives in a timely manner:

- Acquire timely knowledge of Sentinel Events (described in Exhibit A) that may affect the accreditation status of an Accredited Entity or Accreditation Candidate.
- Maintain credibility of DirectTrust as a nationally recognized accreditation body.

Definition

Accreditation "point in time" - Is awarded based upon its review of the organization for that specific "point in time" that the accreditation process occurred. DirectTrust is not responsible for any changes in policies, procedures or controls, processes or access that may occur subsequently in which it has no visibility or is unaware.

Accreditor - DirectTrust provides Accreditations governed by the Electronic Healthcare Network Accreditation Commission (EHNAC) Commissioners, (hereafter, "Accreditor".)

EPCS Aggregator – An EPCS application vendor that integrates their EPCS application within other applications, such as EHR systems developed by other organizations.

Approved by Commission 3/21/23

Breach - The HIPAA Breach Notification Rule – 45 CFR §§ 164.400-414 – requires covered entities and their business associates to report breaches of electronic protected health information and physical copies of protected health information. A breach is defined as the acquisition, access, use, or disclosure of protected health information in a manner not permitted by HIPAA Rules. When the breach has impacted more than 500 individuals, the maximum permitted time for issuing the notification to the HHS is 60 days from the discovery of the breach, although breach notices should be issued without unnecessary delay. In the case of breaches impacting fewer than 500 individuals, HIPAA breach notification requirements are for notifications to be issued to the HHS within 60 days of the end of the calendar year in which the breach was discovered.

Organization – An entity (company, government entity such as an HIE, etc.) seeking accreditation, seeking re-accreditation, or currently accredited by Accreditor.

Accreditor Program – Any of the Accreditation Programs offered by DirectTrust.

In-scope Organization Site – Organization Sites deemed "in scope" are any and all physical locations at which the Accreditor provides services related to the Accreditor Program for which they are seeking/or are currently accredited; and any and all sites that create, receive, maintain, or transmit PHI (Protected Health Information), PII (Personally Identifiable Information), and cryptographic information (e.g., cryptographic keys) related to those services. Services considered in scope include but are not limited to:

1. Data Centers – under all circumstances
2. Network Administration – where necessary to the business for accreditation
3. Customer Service/Helpdesk – where necessary to the business for accreditation
4. DRP Facilities – any functions with access to PHI, PII, or cryptographic information related to DirectTrust accredited services
5. Lockbox Operations– where necessary to the business for accreditation
6. Product Development – where necessary to the business for accreditation
7. Storage Backup – where necessary to the business for accreditation
8. Production Operations – under all circumstances
9. Printing or Scanning operations – where PHI is involved

In-scope Outsourced Site – Outsourced Sites and Service Providers deemed "in scope" are any and all Outsourcers related to the Program for which the Organization is seeking accreditation, or any sites where the Organization's PHI, PII, or cryptographic information (e.g., cryptographic keys) is created, received, maintained, or transmitted. Such sites and services may include but are not limited to:

1. Data Center – under all circumstances
2. Network Administration – where necessary to the business for accreditation
3. Private Cloud – any functions with access to PHI, PII, or cryptographic information related DirectTrust accreditation services
4. Customer Service/Helpdesk – where necessary to the business for accreditation

5. DRP Facilities – any functions with access to PHI, PII, or cryptographic information related to DirectTrust accredited services
6. Lockbox – where necessary to the business for accreditation
7. Product Development – where necessary to the business for accreditation
8. Storage Backup – where necessary to the business for accreditation
9. Production Operations – under all circumstances
10. Printing or Scanning operations – where PHI is involved

Outsourcer – An entity that is contractually obligated to provide services to the Organization.
Outsourced Site – Sites belonging to an Outsourcer.

INTRODUCTION TO SENTINEL EVENTS

1. What is a Sentinel Event?

A Sentinel Event is any significant material impacting development, action or change in the business, financial, operational, organizational or legal status of an entity, which occurs, (1) with respect to an Accredited Entity, after accreditation, or (2) with respect to an Accreditation Candidate, after the application has been submitted to DirectTrust. The material impacting change in status may be based on any one or more of the Sentinel Events indicated below or described in the Sentinel Events Exhibit A.

2. *Notification Process;* When should DirectTrust be notified?

DirectTrust must be notified in writing of the occurrence of any Sentinel Event**. Written notification in the manner described in Section 3 below must be received by DirectTrust no later than three (3) business days from when the Sentinel Event occurs or is reported to a federal/state agency or to the media/press**. Failure to provide such notification could result in loss of Accreditation, loss of Candidacy status or such other action as DirectTrust may determine to be appropriate.

3. How should DirectTrust be notified?

As part of the notification process, the Accredited Entity or Accreditation Candidate shall provide DirectTrust with the "known facts," as determined to have a material impact, and shall continue to provide DirectTrust written notice of additional relevant information as such information becomes "known facts." The additional relevant information shall be delivered to DirectTrust by email sent to admin@DirectTrust.org.

"Known facts" shall include, but not be limited to, (A) any relevant data, information or circumstances regarding a Sentinel Event having a material impact which an Accredited Entity or Accreditation Candidate (i) is required by law, by a contract to which it is a party, or by any other legal obligation to report or disclose to a third party, or (ii) has disclosed in a public statement or in any non-confidential manner; (B) reports or information that must be reported to a government agency and (C) all findings of fact in the form of an agency action by a duly authorized regulatory agency or in a judgment by a court of original jurisdiction, notwithstanding any subsequent appeals.

The written notification should include the following information:

A. Name of the individual reporting the Sentinel Event (company name, individual name, title, address, phone number, and email address).
B. Description of the Sentinel Event.
C. Date the Sentinel Event occurred.
D. DirectTrust Accreditation impact(s) or considerations that could materially and adversely affect the company's compliance with the Accreditation Criteria, e.g., changes in key executive management in a small company or release of a press announcement in a public company.
E. Other factual information DirectTrust should consider.
F. If the Sentinel Event has resulted in non-conformity with the Accreditation Criteria, a proposed plan to restore conformity, i.e., an explanation in reasonable detail of how the company will

promptly reestablish conformity with all applicable Accreditation Criteria.

G. Appropriate documentation should be submitted along with the disclosures, e.g., press releases, etc.

4. What constitutes a Sentinel Event?

The following is an illustrative but not exhaustive topical list of Sentinel Events. Refer to the attached Sentinel Event Exhibit "A" for detailed explanations.

- Entering into an agreement of sale to sell or otherwise directly or indirectly divest an Accredited Entity or an Accreditation Candidate.
- Entering into an agreement to purchase or otherwise directly or indirectly acquire an Accredited Entity or Accreditation Candidate.
- Entering into a new agreement to outsource a site that fits the definition of an In-scope Organization Site or an In-scope Outsourced Site.
- Financial impairment of an Accredited Entity or Accreditation Candidate.
- Insolvency/bankruptcy filing.
- Change in ownership or control> 25%.
- Disruption of service to customers > 8 hours for telecom, or security violation.
- A security/privacy breach that is reportable as a matter of state or federal law. DirectTrust does not warrant that its accreditation framework will prevent any breach or cyberattack. Refer to the HIPAA Breach Definition Notification Rule – 45 CFR §§ 164.400-414.
- Workforce reduction by ≥ 15%.
- Key management changes.
- Company fine(s) of > $100K for regulatory violations, marketing or advertising practices, antitrust violations, or tax disputes.
- Adding or significantly modifying an In-scope Organization Site or an In-scope Outsourced Site.
- Significant events associated with an In-scope Organization Site or an In-scope Outsourced Site including but not limited to the addition or significant modification of physical locations.
- For those certified through an EPCSCP Program, a Sentinel Event must be reported for each significant system upgrade, functional alteration, or when made aware of any application issue related to e-Prescribing in accordance with the regulations. See ***Exhibit A: Sentinel Events, section F. Critical DirectTrust Accredited System Events*** for more information.
- For those certified/accredited through the TDRAAP Program, a Sentinel Event must be reported for each significant change to the product which has been proven via UDAP testing as part of the review process.
- For those accredited through the TNAP-HIN program, a Sentinel Event must be reported if HITRUST certification is not maintained throughout the TNAP-HIN accreditation.
- For those accredited for any program who have been certified by HITRUST and who have used a validated report to satisfy the security or privacy criteria in any DirectTrust program, a Sentinel Event must be reported if HITRUST certification is not maintained throughout the accreditation period.

5. What is the DirectTrust Review Process?

Within seventy-two (72) hours of DirectTrust's receipt of such written notice, the President and CEO of

DirectTrust, if he/she deems the Sentinel Event to be of a materially substantive nature, shall notify the Chair of the Commission and he/she shall convene a meeting of the Ad Hoc Sentinel Event Council Council"), consisting of three EHNAC Commissioners, to consider the matter. In determining its recommended course of action, the Council shall consider the seriousness and time-criticality of the Sentinel Event. The Council shall provide its written recommendation to the Commissioners within twenty-four (24) hours of the conclusion of its meeting, including, if recommended, the necessity for a special meeting of the Commissioners to take action on any recommendation of the Council. Other than the publication of any change to the status of a DirectTrust Accredited Entity or a DirectTrust Accreditation Candidate on the website, all deliberations by DirectTrust on the report of a Sentinel Event, including its evaluation and recommendations, shall be kept confidential. Accreditation by DirectTrust is awarded based upon its review of the organization for that specific "point in time" that the accreditation process occurred DirectTrust is not responsible for any changes in policies, procedures or controls, processes or access that may occur subsequently in which it has no visibility or is unaware. It is the organization's responsibility to report significant changes to us through our Sentinel Events policy.

6. What action may be taken by DirectTrust?

The EHNAC Commissioners shall review the recommendation of the Council on a timely basis, either at a special meeting of the Commissioners if the matter is deemed urgent by the Council's Report, or no later than the next regularly scheduled meeting of the Commission. Written findings and action taken by the Commission shall be communicated in writing to the affected Accredited Entity or Accreditation Candidate within two (2) business days of the conclusion of the meeting of the Commission. The written communication also shall include a description of DirectTrust's appeal procedures.

The following are examples, illustrative but not comprehensive, of actions that may be taken by the Commission:

- No action.
- Revocation of accreditation.
- Request for further documentation. If the additional documentation is not provided, revocation of accreditation.
- Request the organization to reapply and follow the re-accreditation process if it is determined that the Sentinel Event provides a substantive change to the entity. Such other actions as are deemed appropriate.
- Change in Accreditation Status
- Please note: if an organization fails to respond to a high priority email from DirectTrust within 7 business days indicating their intention to proceed with the accreditation process then DirectTrust will make the determination that the organization no longer intends to maintain their accreditation status and will be removed from the website and the organization will no longer be accredited on that date.

7. Public Posting

Any change in Accreditation status pertaining to the Accredited Entity or Accreditation Candidate shall be posted on the DirectTrust and/or EHNAC website.

8. Significant Events Other Than Sentinel Events

If one or more of the following occur(s) within 12 months of the last accreditation, a site visit must be made to the new or modified facility (ies):

- Accredited Entity enters into a new agreement with an In-scope Outsourced Site.
- Accredited Entity adds or significantly modifies a physical location that would qualify as an In-scope Organization Site or an In-scope Outsourced Site.
- A significant event occurs associated with functions involving the creation, reception, maintenance, or transmission of PHI that are outsourced to third parties including but not limited to their addition or significant modification of physical locations.
- Increasing the level of identity or authentication assurance supported by a TDRAAP accredited program
- A notifiable breach. (Refer to the Breach Definition and the HIPAA Breach Notification Rule – 45 CFR §§ 164.400-414)

If the Significant Event occurs after 12 months past the last accreditation, a site visit may be made to the new or modified facility(ies) if determined to be necessary by DirectTrust. If decided a site visit is necessary, the information gathered will be applied to the subsequent accreditation effort and reports accordingly.

NOTE: *A change in the organizations contact individual having responsibility to liaison with DirectTrust needs to be communicated within 10 days of a change in personnel so that there is no disruption in any notices or communications between the entities.*

EXHIBIT A

SENTINEL EVENTS

A list of Sentinel Events is presented below. An answer of *YES* by an Accredited Entity or Accreditation Candidate to any question in the list triggers DirectTrust's *Notification Process*.

In reviewing the list, remember that in circumstances where an Accredited Entity or Accreditation Candidate is a division or subsidiary of a parent organization, Sentinel Events occurring at the parent organization level are subject to the same *Notification Process* to enable DirectTrust to review the Sentinel Event to determine if it is material to the Accredited Entity or Accreditation Candidate.

A. ACQUISITION OF ANOTHER ENTITY OR SALE OF AN ENTITY OR SUBSIDIARY(IES)

1. Has the Accredited Entity or Accreditation Candidate entered into a binding agreement to acquire, directly or indirectly, another organization, which is involved in any activity directly related to the accreditation status of the Accredited Entity or the Accreditation Candidate regardless of whether the acquired entity is accredited by DirectTrust?
2. Has the Accredited Entity or Accreditation Candidate entered into a binding agreement to sell, divest, or otherwise transfer control of any part of its accredited business (or the business for which it seeks accreditation) to another entity? (This could be a department, unit, subsidiary(s), etc.)
3. Has the Accredited Entity or Accreditation Candidate undertaken a change of control and/or name change or are there other areas or new areas (or entities) within the organization that now need to be reviewed under current or other DirectTrust programs in order to be compliant with DirectTrust Accreditation Criteria? If yes, those areas or entities will need to be defined and a formal "plan of action" submitted to DirectTrust related to achieving compliance within a maximum one-year timeframe. During this time the accreditation status will change to Interim Accreditation.

B. EVENTS OF DEFAULT OR INSOLVENCY

1. Has the Accredited Entity or Accreditation Candidate incurred or otherwise suffered an adverse financial event that has the potential to materially and adversely affect its ability to maintain its current level of accredited business operations consistently and without prolonged interruption?
2. Has the Accredited Entity or Accreditation Candidate become insolvent, or has it suffered or consented to, or applied for, the appointment of a receiver, trustee, custodian, or liquidator of itself or any of its property, or has it generally failed to pay its debts as they become due, or has it made a general assignment for the benefit of creditors?
3. Has the Accredited Entity or Accreditation Candidate filed a voluntary petition in bankruptcy, or is it seeking reorganization, in order to effect a plan or other arrangement with creditors or any other relief under the Bankruptcy Reform Act, Title 11 of the United States Code, as amended or recodified from time to time ("Bankruptcy Code"), or under any state or federal law granting relief to debtors,

whether now or hereafter in effect; or has any involuntary petition or proceeding pursuant to the Bankruptcy Code or any other applicable state or federal law relating to bankruptcy, reorganization or other relief for debtors been filed or commenced against the Accredited Entity or Accreditation Candidate; or has the Accredited Entity or Accreditation Candidate been adjudicated a bankrupt, or has an order for relief has been entered against the Accredited Entity or Accreditation Candidate by any court of competent jurisdiction under the Bankruptcy Code or any other applicable state or federal law relating to bankruptcy, reorganization or other relief for debtors?

4. Has any director, stockholder or member taken action seeking to effectuate the dissolution or liquidation of the Accredited Entity or Accreditation Candidate?
5. Has any direct or indirect change in ownership or control occurred whereby, in the aggregate, more than twenty-five percent (25%) of the common stock or other equitable interest in the Accredited Entity or Accreditation Candidate has changed hands?

C. OPERATIONAL SERVICE EVENTS

1. Has the Accredited Entity or Accreditation Candidate experienced a disruption in telecommunications or other core communications technology (e.g., ASP) greater than 8 hours unrelated to a natural disaster?
2. Has the Accredited Entity or Accreditation Candidate experienced a disruption of HIE and/or EMR services that extend beyond Service Level Agreement (SLA) or DirectTrust Program requirements or other pre-announced maintenance windows?
3. Has the Accredited Entity or Accreditation Candidate experienced a disruption in service to customers greater than 8 hours related to a material security incident or software virus?
4. Has the Accredited Entity or Accreditation Candidate reduced its workforce by 15% or more within any twelve (12) month period, or has it announced plans for any other workforce reductions that may be reasonably expected to impact the ability of the Accredited Entity or Accreditation Candidate to continue to comply with Accreditation Criteria?
5. Has the Accredited Entity or Accreditation Candidate experienced any changes in key management personnel, i.e., president or above or has any such change occurred within the parent company or any affiliate covered by DirectTrust accreditation?
6. Has the Accredited Entity or Accreditation Candidate reported or experienced a privacy or security breach that is reportable for any reason to any person pursuant to the laws of any state or federal that may apply to the Accredited Entity or Accreditation Candidate?
7. Has the Accredited Entity or Accreditation Candidate added or significantly modified a physical location in the company that provides a function described in the definition of In-Scope Organization Site?
8. Has the Accredited Entity or Accreditation Candidate lost HITRUST certification status resulting in the nullification of security or privacy criteria evidence that was relied-upon for DirectTrust Accreditation?

D. EVENTS RELATED TO IN-SCOPE OUTSOURCED SITES

1. Has a decision been made to outsource a function described by the definition of In-scope Organization Site? Such decision must be reported prior to the time the function is outsourced.
2. Has a decision been made to change vendors performing a function described by In-scope Outsourced Site? Such decision must be reported prior to the time the vendor conversion is completed.
3. Has any In-scope Outsourced Site committed a material breach of contract, including any disclosure of PHI? Such a breach must be reported within 30 days of the discovery of the breach.
4. Has a decision been made to bring in house a function described by the definition of In-scope Outsourced Site that was previously outsourced? Such decision must be reported prior to the time that function is brought in house.
5. Has an In-scope Outsourced Site added or significantly modified any of its physical locations in which it provides in-scope services? Such changes must be reported as soon as they are known.

E. BUSINESS PRACTICE EVENTS

1. Has the DirectTrust Accredited Entity or Accreditation Candidate been accused of an event for which it may be subject to a governmental consent order or decree or may be ordered to pay fines or civil penalties greater than $100,000 by a third party in either a non-governmental arbitration or judicial cause of action related to a breach in security, confidentiality, or privacy of any individually identifiable healthcare data?
2. Has such an order, fine or penalty been issued related to a breach in security, confidentiality, or privacy of any individually identifiable healthcare data, even if under appeal?
3. Has the DirectTrust Accredited Entity or Accreditation Candidate been notified by a federal or state government agency that it must submit a plan of correction or pay a civil monetary penalty or fine for failure to comply with any applicable rule or regulation relating to standard transactions, code sets, unique identifiers, or regulations concerning the privacy or security of electronic information?

F. CRITICAL DIRECTTRUST ACCREDITED SYSTEM EVENTS

Some DirectTrust programs accredit specific services rather than organizations. These include the EPCSCP and PMSAP programs.

1. For EPCSCP programs, a sentinel event must be declared whenever, as stated in 21 C.F.R. § 1311.300(a), a functionality related to controlled substance prescription requirements is altered.
2. For EPCSCP programs, a sentinel event must be declared when the following occurs: As stated in 21 C.F.R. § 1311.302(a), the application provider must, in the event that the application provider identifies or is made aware of any issue with its application that make the application non-compliant with the requirements of § 1311, notify practitioners or pharmacies that use the application that the application should not be used to issue or process electronic controlled substance prescriptions.

Such notification should take place as soon as feasible, but no later than five business days after discovery.

3. For all DirectTrust accredited systems, a sentinel event must be declared whenever a substantive system update is ready to be deployed. This must include at a minimum each major release of the software.
4. An EPCS Aggregator (see Definitions) must declare a Sentinel Event when an organization desires to bring a new application live that uses the EPCS Aggregator's software. Surescripts requires a third-party audit of such implementation, which DirectTrust provides (with fee) to its EPCS Accredited organizations that act as EPCS Aggregators.

I have reviewed the above DirectTrust Business Risk Planning and Sentinel Events and agree to comply.

Signed: _____

Print Name: _____

Title: _____

Company: _____

Date: _____