

## 1 Purpose

The purpose of this procedure is to ensure that individual protected health information (PHI) is handled properly when such information is required to provide contracted services to CliniComp, Intl.'s (hereafter referred to as CCI) customers, and to ensure that CCI complies with obligations under the Business Associate Agreements with customers and applicable laws, regulations, and guidelines. With respect to safeguarding PHI, this policy overrides and governs any other general policy documents or other standard operating procedures.

## 2 Scope

Generally, by the nature of the CCI software solution (Clinical Information System [CIS]) and services provided to customers, this policy addresses the two predominant sources of PHI encountered by CCI workforce:

- 2.1 Access to PHI in a CIS located at customer site
- 2.2 Access to PHI in the CCI tracking solution, ServiceDirect, located internally at CCI facility.
- 2.3 This procedure is not applicable to other employment information regarding CCI employees.
- 2.4 This policy applies to all members of CCI's workforce.

## 3 References

DOCUMENT NO.	TITLE
Title 45 CFR Part 164.530	"Security and Privacy Administrative Requirements," Aug. 2002.
Privacy Act 1974	HIPAA Privacy Act 1996; HIPAA Security Rule 1998
HIPAA Administrative Simplification	Regulation Text, U.S. Department of Health and Human Services Office for Civil Rights, Feb. 16, 2006.
HIPAA Privacy Rule	HIPAA Compliance Assistance, OCR Privacy Rule Summary, 05/03.
45 C.F.R. parts 160 and 164	Standards for Privacy of Individually Identifiable Health Information and Security Standards for the Protection of Electronic Protected Health Information. Health Information Technology for Economic and Clinical Health Act ("HITECH" Act), as may be amended from time to time.
	VA Cyber-Security Requirements
DoD 5200.1-R	"Department of Defense Information Security Program Regulation," January 17, 1997.
DoD Directive 5200.1	"DoD Information Security Program," December 13, 1996.
DoD Instruction 8500.2	"Information Assurance (IA) Implementation," February 6, 2003.
DoD Directive 8500.01	"Information Assurance (IA)," October 24, 2002.

DOCUMENT NO.	TITLE
SE0006	CCI Password Policy
SE0010	Information Systems Use Policy
SE0014	CCI Physical and Environment Controls Policy
SE0023	CliniComp's DoD Cybersecurity Policy
254-70028	ServiceDirect Internal User Guide

## 4 Responsibility

ROLE	RESPONSIBILITY
CCI Management	<ul style="list-style-type: none"> <li>Responsible for implementing and assuring adherence to this policy.</li> </ul>
CCI Workforce	<ul style="list-style-type: none"> <li>All members of CCI's workforce are responsible for awareness of this policy, to ensure protection of PHI from unauthorized access, use, or disclosure, by adhering to this policy, and for reporting known or suspected violations.</li> </ul>
Privacy Officer	<ul style="list-style-type: none"> <li>Chief Executive Officer (CEO) appoints the Privacy Officer and records the designation in writing. Because CCI's need for access to and possession of PHI is limited and controlled, the position of Privacy Officer is not a full-time requirement and tasks assigned to the Privacy Officer are collateral to the appointee's general work activities. The Privacy Officer will report to the Chief Executive Officer with respect to matters involving PHI concerns only, and otherwise will continue to report to his or her designated departmental manager or, if applicable, executive management, for all of his or her normal activities.</li> <li>Whenever in this policy reference is made to the Privacy Officer's "responsibility" or "authority", those references are not to be construed as requiring or empowering unilateral action or decision making by the Privacy Officer, but, instead, mean the Privacy Officer:               <ol style="list-style-type: none"> <li>takes the lead and has authority for general oversight of the workforce activities and practices relating to or impacting the protection of privacy interests, including identification and investigation of workforce activities and other practices that result in a violation or portend a significant risk of violation of privacy protections,</li> <li>is the designated Point of Contact for:                   <ol style="list-style-type: none"> <li>receiving and managing complaints (whether from other workforce members or customers) concerning workforce activities relating to privacy interests,</li> </ol> </li> </ol> </li> </ul>

ROLE	RESPONSIBILITY
	<ul style="list-style-type: none"> <li>ii. fielding and arranging for responses to workforce questions concerning privacy interests, or arranging for the proper record management of PHI received from a customer or other source,</li> <li>iii. generally coordinating with and receiving information from other workforce members having direct responsibility for physical and technical security for CCI's facility and equipment with respect to matters concerning protection of privacy interests.</li> <li>c. reports and makes recommendations to Compliance leadership with respect to such matters and others that concern privacy interests, including reporting and making recommendation for enforcement actions; and</li> <li>d. participates in implementation of decisions made by Compliance leadership, or, when appropriate, in conjunction with other member of executive management, and taking the lead in overseeing and evaluating and reporting on such implementation and its effectiveness.</li> </ul> <ul style="list-style-type: none"> <li>• Ensure he or she receives training and periodic refresher courses to ensure compliance with privacy guidelines and reporting process.</li> <li>• Will oversee job-specific workforce training related to the protection of privacy, with such training to be updated as needed over time, and renewed for all workforce on an annual basis</li> </ul>

## 5 Definitions/Acronyms

TERM	DEFINITION
Breach	The acquisition, access, use, or disclosure of protected health information in a manner not permitted under 45CFR §§164.500-534, which compromises the security or privacy of the protected health information: (1)(i) For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual. (ii) A use or disclosure of protected health information that does not include the identifiers listed at §164.514(e) (2) date of birth, and zip code does not compromise the security or privacy of the protected health information.
Business Associate	A person or organization under written contract, other than a member of a Covered Entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a Covered Entity that involves the use or disclosure of individually identifiable health information.

TERM	DEFINITION
Clinical Information System (CIS)	A comprehensive, integrated computer hardware and software system used for the capture, review, and management of patient clinical documentation at a Covered Entity (i.e. hospital or other inpatient facility).
Covered Entity	Healthcare providers, health plans, and healthcare clearing houses that transmit health information in electronic form in connection with transactions for which the Secretary of the Department of Health and Human Services has adopted standards.
Disclosure	The release, transfer, provision of, access to, or divulging in any other manner of PHI outside the entity holding the information.
De-identified Health Information	PHI that has been altered by the removal of specified identifiers of the individual and the individual’s relatives, household members, and employers so that the remaining information cannot be used to identify the individual. De-identified health information neither identifies nor provides a reasonable basis to identify an individual.
HIPAA	Health Information Portability and Accountability Act of 1996 and the regulations and guidance promulgated thereunder by the Department of Health and Human Services.
HITECH Act	Health Information Technology for Economic and Clinical Health Act of 2009 and the regulations and guidance promulgated thereunder by the Department of Health and Human Services.
Incident	Any physical, technical, or personal activity or event that increases the risk to inappropriate or unauthorized use or disclosure of PHI or causes non-compliance to this policy and provisions of HIPAA.
Individually Identifiable Health Information (II)	Information, including demographic information, created by a Covered Entity, that relates to the past, present or future physical or mental health or condition of the individual; the provision of healthcare to an individual; or the past, present or future payment for the provision of healthcare to an individual, that identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
Live Site	A customer site with an operational CIS containing actual patient data including PHI.
Protected Health Information (PHI)	All individually identifiable health information maintained or transmitted by a Covered Entity or its Business Associate, in any form or medium (e.g., electronic, paper, or oral).
Support Perimeter	Secured area at CCI headquarters housing clinical support personnel and CCI support equipment and facilities utilized to access CIS systems at customer sites.
Support Personnel	CCI employees and contractors with role-based privileges that have a bona fide need to access a live site.

TERM	DEFINITION
ServiceDirect	A customized portal allowing both CCI staff and customers to track issues, such as CIS installation projects, customer support issues, etc. Customers can only see tickets for their site(s). Each ServiceDirect ticket can have one or more documents attached
Suspected Violations	Suspected violations of PHI access, use, or disclosure will be reported to the Privacy Officer and through the reporting process described in this policy to include investigation, mitigation, and development of an action plan, as appropriate.
Unsecured Protected Health Information	PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5 on the HHS Web site.
Use	With respect to PHI, the sharing, employment, application, utilization, examination, or analysis of such PHI within the entity’s internal operations.
Workforce	Employees (whether part-time, full-time or temporary), contractors, interns, students, trainees, and other persons whose conduct, in the performance of work for CCI, is under the direct control of CCI.

## 6 Attachments/Appendixes

- 6.1 Attachment A: Privacy Officer Appointment
- 6.2 Attachment B: De-identification of CIS PHI
- 6.3 Attachment C: Transmittal Sheet

## 7 General Information

### 7.1 Policy Document Organization

7.1.1 Appropriate administrative, technical, and physical safeguards exist at CCI that reasonably and appropriately protect the confidentiality, integrity, and availability of PHI from any intentional or unintentional use or disclosure that violates HIPAA rules and provide a reasonable effort to limit the use or disclosure of (and requests for) PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. References in this policy to “privacy,” “privacy interests,” or similar terms mean only privacy of a customer’s PHI and this policy does not apply to other types of privacy concerns, such as employment information concerning CCI employees, etc.

7.1.2 Additionally, this policy is organized into the following two sections to address the two sources of PHI typically encountered by CCI workforce, as follows:

- 8.1 Procedure – PHI in the CIS
- 8.2 Procedure – PHI in Service Direct

## 7.2 Administrative Measures

### 7.2.1 Infractions, Disciplinary Actions, Sanctions, and Fines

- 7.2.1.1 In extending important HIPAA duties to Business Associates, the HITECH Act imposed certain procedural requirements on Business Associates like CCI, including a requirement to maintain a reasonable system of discipline or sanctions for violations by its workforce.
- 7.2.1.2 CCI workforce members shall be responsible for maintaining the confidentiality of any PHI entrusted to them and for reporting known or suspected violations (i.e., unauthorized access, use, or disclosure of PHI), whether by the reporting workforce members, others in the workforce, or by persons acting on behalf of the Covered Entity (i.e., hospitals employees involved with the support issue).
- 7.2.1.3 Violations of this policy or applicable legal requirements for protection of PHI will be subject to corrective disciplinary action by CCI, up to and including termination.
- 7.2.1.4 Corrective action includes but is not limited to: training; coaching; retraining; informal counseling; formal counseling; final counseling; suspension; demotion or termination /dismissal. Corrective action must comply with the provisions of applicable federal and state laws and regulations, CCI policies, and any other applicable documents or agreements related to the workforce members' status as an employee.
- 7.2.1.5 The CCI Privacy Officer is responsible for evaluating, developing, and implementing corrective action in consultation with Compliance leadership, People Operations, and in case of termination, the CEO.
- 7.2.1.6 Under the HITECH Act, employees willful or reckless violations can result in fines and penalties for CCI and the involved individual, and in extremes case of egregious violations for commercial exploitation or other illicit purpose, criminal prosecution sanction and incarceration.

### 7.2.2 HIPAA and PHI Training

- 7.2.2.1 All members of CCI's workforce, including contract workers and student interns, shall undergo CCI-specific HIPAA and PHI

training, demonstrate proof of understanding, and sign an agreement to comply with this policy and all HIPAA regulations before access or exposure to PHI information that may include PHI. Annual refresher training and review also is required. Workforce members who support Department of Defense (DoD) customers shall have additional training and compliance requirements. Training will include:

- In-service training on PHI and HIPAA regulations regarding access to, and use and disclosure of, such data.
- Education on the legitimate grounds for initiating remote CIS access.
- Education on site-specific requirements concerning security, privacy, or support in general.
- Ongoing training as system software, hardware, and responsibilities evolve.
- Annual refresher courses.

**7.2.2.2** Record of Training. The People Operations department shall maintain records of training and agreement for compliance.

### **7.2.3** Handling Investigations

**7.2.3.1** Within 24 hours of becoming aware of a PHI incident, either an actual breach or suspected violation, the Privacy Officer shall notify Compliance leadership, who will:

- a. in the case of an actual breach, Compliance leadership, will notify the appropriate representative of the impacted Covered Entity, and
- b. in the case of a suspected violation, proceed, in collaboration with the Privacy Officer, to investigate and determine if the suspected violation in fact occurred and if so, proceed with notification to the Covered Entity.

**7.2.3.2** When notification to the Covered Entity is required, such notification will be made within one business day of the determination of a breach or violation, but in no event longer than five days after becoming aware of the breach or confirmed violation; provided, however, if a shorter initial notification period is required under any customer contract, then notice shall be given in accordance with the applicable contract requirement.

- 7.2.3.3 Within ten business days of an initial notification of such incident, a written report of the incident shall be submitted to the appropriate representative of the impacted Covered Entity. This report shall include:
- A detailed description of the incident,
  - The mitigation procedures that were implemented to lessen its impact, and
  - The processes (reasonable and appropriate) safeguards that were established to prevent the incident from reoccurring.
  - The report should not disclose or repeat PHI, provided if PHI is essential to understanding the report, then transmittal of the report shall only be made by secure delivery means as described below.
- 7.2.3.4 When an incident concerns or involves a CCI workforce member, if appropriate, the Privacy Officer will notify the workforce member's manager about the nature of the incident. Notification includes a description of the process and expected timeline for completion of the investigation.
- 7.2.3.5 All incident investigations are documented and tracked in CCI's ServiceDirect. In general, compliance investigation records are retained in accordance with the record management and retention policy applicable to ServiceDirect. An exception is with paper documents concerning investigations (with any PHI redacted or otherwise secured), which also may be retained by the Privacy Officer, the Compliance leadership, or the CEO, when necessary for compliance with legal processes, and such records shall be retained in a secure manner with other confidential legal documents.

## 8 Procedure

### 8.1 PHI in a CIS

#### 8.1.1 Administrative Safeguards

##### 8.1.1.1 Access Controls for PHI in a CIS

- 8.1.1.1.1 CIS access at a live site is granted only to support personnel who are HIPAA trained with validation and have a role-based privilege that requires CIS access in performance of work-related duties.



- 8.1.1.1.2** CIS PHI at a customer site is strictly confidential. Support personnel shall have access to PHI in a CIS for the following uses:
- Service/repair/identify CIS problems as reported by the CCI auto-page system or by hospital personnel.
  - Ensure date accuracy for clinical decision-making (e.g., conduct quality assurance activities).
  - Test configurations for the CIS.
  - Perform software development, maintenance, and implement installations on the CIS.
  - Retrieve CIS data as requested by customer.
  - Assist user with documentation questions during go-live support.
  - Other uses expressly authorized in writing by CCI executive management, with customer permission.
- 8.1.1.1.3** CCI does not use real customer PHI for sales, marketing, demonstrations, training, or testing purposes.
- 8.1.1.1.4** No PHI shall be removed or transmitted beyond CCI's secured area.

## **8.1.2** Physical Safeguards

### **8.1.2.1** Facility Controls for PHI in a CIS

- 8.1.2.1.1** The CCI building and CIS support perimeter shall be locked 24 hours a day, seven days a week. Physical access to the CCI building and co-location site shall be restricted to CCI workforce members via access code-controlled entry. All others wishing to enter the facility must be granted access by CCI staff. Once in the building, the individual shall be required to sign a visitor's log, obtain a visitors' badge, and be escorted during their stay. Any unescorted visitors should be stopped, questioned, and escorted accordingly.
- 8.1.2.1.2** All CCI building and CIS support perimeter successful and unsuccessful access attempts are logged and reviewed monthly.

#### 8.1.2.2 Media Controls for PHI in a CIS

8.1.2.2.1 Only de-identified CIS data shall be removed from the CCI support perimeter or placed on a removable media by CCI workforce members.

#### 8.1.3 Technical Safeguards

##### 8.1.3.1 Remote Access Controls for PHI in A CIS

8.1.3.1.1 Remote access to a CIS from CCI headquarters is achieved using IPsec virtual private network (VPN) technology. This technology is used to establish a secure connectivity tunnel between secure workstations and servers located in the CIS support perimeter and the customer sites.

8.1.3.1.2 After hours support shall be performed by trained and authorized support personnel located either physically within the CIS support perimeter or accessing resources located within the CIS support perimeter via an IPsec VPN connection established from their CCI-provided secure workstation. VPN access shall be restricted by:

- A unique system login/password scheme to control access to support the CIS.
- Logins shall be validated against a list of currently authorized support logins.
- Login attempts shall be logged to a file, whether validation succeeds or fails.

8.1.3.1.3 For the complete set of technical safeguards in place, refer to SE0014 Physical and Environment Controls Policy, SE0010 Information Systems Use Policy, and SE0023 CliniComp's DoD Cybersecurity Policy.

#### 8.1.4 Procedure for handling PHI in a CIS

##### 8.1.4.1 Use of De-identification CIS Data

8.1.4.1.1 De-identification procedures for PHI requires the removal of any identifiers as described in 45 CFR §164.514, including the identifiers of the patient or of the patient's relatives, employers, or household members (See Attachment B "De-identification of CIS PHI").

- 8.1.4.1.2** It is recommended that the customer site providing the source information de-identify PHI before transferring data to CCI. When the site does so, CCI will confirm in writing the de-identification of sent information. If the customer site (or a Business Associate Agreement with the customer) authorizes CCI to de-identify the data, CCI will remove the PHI identifiers listed above using CCI methodology.
- 8.1.4.1.3** When the site (or a Business Associate Agreement) authorizes CCI to de-identify data, de-identification will take place upon receipt by CCI and prior to use or disclosure of the data for any purpose other than uses or disclosures authorized for PHI under HIPAA and the applicable Business Associate Agreement.
- 8.1.4.1.4** If substitute names and/or numbers are needed in the de-identification process, replacement naming and numbering conventions will be used. These conventions will use an obvious sequential method for applying the substitute name or number, so that an observer could easily identify the convention applied.
- 8.1.4.1.5** When CCI is assisting a customer site with research involving patient data, the customer is responsible for ensuring de-identification of PHI and re-identification, if necessary.
- 8.1.4.1.6** In unique situations, with the written agreement of the customer, information may be de-identified using the alternative technique specified in HIPAA regulation 42 CFR § 164.524(b)(1), which permits the custom design of a de-identification process based on an opinion from an expert, as described in such section.
- 8.1.4.1.7** With the approval of executive management, CCI may enter into a Data Use Agreement with a customer for the use of PHI for research, public health, or healthcare operations purposes, subject to the terms of such agreement and HIPAA.

## 8.2 PHI in ServiceDirect

**8.2.1** Customers may use PHI when reporting a technical issue; PHI may be received in via email, fax, or postal mail. CCI's policy is to ensure all PHI in its possession is quickly and securely moved to the ServiceDirect portal where it can be held and managed securely. CCI's Privacy Officer should be notified immediately if workforce members received PHI via unencrypted email or facsimile. In the case of facsimiles, the facsimile hard drive will be cleared immediately. The policies and procedures in this section work to ensure that all PHI is routed to the ServiceDirect portal, and it is properly identified and held securely once isolated within ServiceDirect using robust administrative, technical, and physical safeguards.

### 8.2.1.1 Administrative Safeguards

#### 8.2.1.1.1 Access Controls for PHI in ServiceDirect

**8.2.1.1.2** ServiceDirect is the designated repository for all PHI received by CCI from a customer or any other source.

**8.2.1.1.3** While most CCI workforce members have access to ServiceDirect, access to PHI in ServiceDirect is granted on a "need to know" basis. Only those CCI workforce individuals who are HIPAA trained per this policy and specifically require access to the PHI in ServiceDirect in order to perform their work-related duties are granted such access.

**8.2.1.1.4** PHI in ServiceDirect is strictly confidential. The only acceptable purpose of accessing PHI in ServiceDirect is when such access is directly necessary in order to troubleshoot, service, repair, identify, or document CIS support issues.

**8.2.1.1.5** No PHI shall be removed or transmitted beyond CCI's secured area. If a workforce member receives a request to release any PHI to a third party, the member will refer the request to the Privacy Officer for resolution.

### 8.2.1.2 Record Management of PHI Data in ServiceDirect

**8.2.1.2.1** Any PHI received by means or media other than by a customer inserting it into ServiceDirect shall be deposited into ServiceDirect with the original PHI

data appropriately destroyed and such destruction commented in the applicable ServiceDirect log.

- 8.2.1.2.2 Workforce members shall comply with the published rules and instructions pertaining to the method of maintaining PHI in ServiceDirect records, and each is affirmatively tasked with correcting any errors identified in any record whether or not he or she generated the particular record or PHI entry.
- 8.2.1.2.3 Questions concerning use of ServiceDirect should be directed to the ServiceDirect Manager designed by Engineering; however, concerns relating to PHI in ServiceDirect should be directed to the Privacy Officer.
- 8.2.1.2.4 Generally, ServiceDirect records (including those containing PHI) shall be retained indefinitely until otherwise directed by executive management; provided, however, in no event, shall the period of retention be less than the minimum period required by law.
- 8.2.1.2.5 Generally, requests from a customer requesting destruction of PHI will be accommodated, except with respect to records concerning the FMRD (required to be retained in accordance with FDA requirements) or records subject to some known legal process (exception pending legal process and FMRD). Any requests from a customer requesting destruction of PHI in a ServiceDirect record shall be referred to the Privacy Officer and the referring workforce member should advise the customer of such referral and the contact information for the Privacy Officer.

## 8.2.2 Physical Safeguards

### 8.2.2.1 Physical Security

- 8.2.2.1.1 Physical security measures at CCI exist to control access to key assets including the ServiceDirect system. The ServiceDirect server is housed in the CCI Data Center, which maintains an additional layer of biometric security on top of the existing facility access security. The policy SE0014 CCI Physical and

Environment Controls Policy further stipulates the security means in place.

#### 8.2.2.2 Media Controls for PHI in ServiceDirect

8.2.2.2.1 PHI shall be attached electronically as isolated PHI within ServiceDirect.

8.2.2.2.2 PHI not located in ServiceDirect shall be shredded and not copied, scanned, faxed, or emailed, with the single exception that PHI shall be scanned into ServiceDirect.

8.2.2.2.3 PHI in ServiceDirect shall NOT be copied onto an archive or removable medium with the single exception of the encrypted backup media stored securely within CCI and/or transferred to the secure offsite storage service provider with whom CCI has contracted.

#### 8.2.3 Technical Safeguards

##### 8.2.3.1 System Access Controls for phi in servicedirect

8.2.3.1.1 Access to PHI located in ServiceDirect is restricted by:

- An authentication (login/password) and authorization scheme to control access to ServiceDirect.
- A specific PHI authorization made available to only those individuals who require it. ServiceDirect automatically limits access to any item flagged as containing customer site PHI to only authorized workforce members, who have a demonstrable need for access for purposes of carrying out their assigned task responsibilities.
- Logins are validated against a list of currently authorized logins.
- Login are logged to a file, whether validation succeeds or fails.

8.2.3.1.2 Further, access to ServiceDirect by CCI workforce members is predicated on access into the CCI building (as authenticated via keypads with individual key codes) and/or CCI corporate username and password authentication into via secure VPN for remote users.

#### 8.2.4 Procedure for handling PHI in ServiceDirect

##### 8.2.4.1 Workforce management of discovered data resembling PHI

If a workforce member comes into contact with data, in any format, which resembles PHI, and this data is not being used in the performance of his or her work, he or she is obligated to complete the following steps:

1. Secure the PHI so that it is not available to others.
  - If it is hard copy (e.g., mail, faxed document), place in a folder or envelope. Do not make copies.
  - If it is electronic (e.g., email), do not forward to anyone. Do not send electronic copies of any questionable data or make electronic reference by email or otherwise to such data, unless directed to do so by executive management.
    - o Perform the following: open a new ServiceDirect and attach the electronic information as an attachment (not in the ServiceDirect comment area). Be sure to properly record the sender/originator. Mark the ServiceDirect ticket as “Contains PHI” and direct it to the Privacy Officer. DO NOT otherwise forward the information to anyone, DO NOT reply to the email, and do not reference the email in another email. Once all the information is in ServiceDirect, delete the original electronic copy (email, file, etc.) from the transmitted system, and log this deletion in the ServiceDirect ticket.
    - o For any questions on using ServiceDirect, refer to ServiceDirect Internal User Guide or contact the ServiceDirect Manager.
  - If it is received as a comment or attachment in ServiceDirect, ALWAYS select the “Contains PHI” check box for that comment entry.
  - Do NOT conduct an investigation regarding the PHI as an investigation may constitute a HIPAA violation.
2. Isolate the PHI to the authorized individual.
  - If it is received by hand delivery, in the mail (regular or express) or by facsimile transmission, provide the hard copy (including any correspondence and the envelope if available) to the Privacy Officer for appropriate disposition – DO NOT MAKE COPIES.
    - o The Privacy Officer scans the PHI into electronic form, attaches the electronic PHI to a new or existing ServiceDirect comment, verifies the ServiceDirect comment is checked as PHI, and records the destruction in the ServiceDirect record.

- o The Privacy Officer shreds any hard copy versions of PHI.
- o The Privacy Officer ensures that any scanner / printer with memory has its memory flushed, so that no further copies may be produced.
- For PHI received through mail, fax, and email, the CCI Privacy Officer notifies sender of PHI to not send PHI through those means.
- Report the situation personally or by phone to the Privacy Officer. If the Privacy Officer is not readily available, report the situation to the Compliance leadership or the CEO. The workforce member's supervisor may assist the workforce member in making such reports if the workforce member desires.

#### 8.2.4.2 Secured Means of Transmitting data resembling PHI

From time to time, it may be necessary for PHI to be transmitted from CCI, such as the specific request of a customer and/or in the context of a legal procedure or process. The following measures shall be followed in this case:


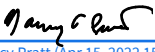

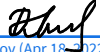
- The Privacy Officer shall be the only person authorized to perform or approve PHI transmission from CCI.
- NEVER send PHI in an EMAIL or attached to an EMAIL.
- In the case where the Covered Entity representative is asking to view PHI in ServiceDirect, if feasible, grant the Covered Entity representative temporary, secure access to the PHI located in ServiceDirect.
- If information must be transmitted by fax, and such transmittal has been approved by the Privacy Officer, always use a fax transmittal sheet identifying specific recipient and including the CCI approved confidentiality notice (See Attachment "Fax Cover Form"). Prior to transmission, contact the recipient and have him or her stand by the fax. Be sure to confirm receipt of fax. Shred the faxed source materials.
- Use certified mail or a reputable courier service. Address the package to a specific, named recipient, and obtain confirmation directly from the recipient that the package has been received.



## 9 Revision History

REV	ORIGINATOR	REFERENCES	EFFECTIVE DATE	DESCRIPTION OF CHANGE
A	N/A	N/A	26 Apr 2000	First Issue of new document
B	N/A	N/A	24 Oct 2000	Correct policy number to appropriate classification
B	N/A	N/A	24 Oct 2000	Management Review, 09/2/04
C	N/A	N/A	02 Apr 2008	Policy Rewrite
D	N/A	N/A	06 May 2010	Update to new template
E	N/A	N/A	16 Nov 2010	Policy renamed and updated per HITECH Act
F	N/A	N/A	12 Dec 2011	Update to privacy officer; Change compliance VP to Compliance Leadership
F	T. Diaz	N/A	12 Dec 2011	Administrative change to reflect annual review, 09/22/20. No document update needed
F	K. Hanten	N/A	12 Dec 2011	Administrative change: updated to new template, 3/25/22
G	D. Lyakov	DCO-00012	18-Apr-2022	Annual Review. Minor updates to reflect the current company process.

## 10 Approvals (for Regulatory Use Only)

<b>AUTHOR</b>	 <a href="#">Dessi Lyakov (Apr 15, 2022 14:45 PDT)</a> Adobe Acrobat Sign Transaction Number: CBJCHBCAABAIRD5q7eTRfLBubPAIL11efeDTyujTftb
<b>DEPT. APPROVAL</b>	 <a href="#">Nancy Pratt (Apr 15, 2022 15:58 PDT)</a> Adobe Acrobat Sign Transaction Number: CBJCHBCAABAIRD5q7eTRfLBubPAIL11efeDTyujTftb
<b>CYBERSECURITY APPROVAL</b>	 <a href="#">Brian Rowe (Apr 18, 2022 14:33 PDT)</a> Adobe Acrobat Sign Transaction Number: CBJCHBCAABAIRD5q7eTRfLBubPAIL11efeDTyujTftb
<b>REGULATORY APPROVAL</b>	 <a href="#">Dessi Lyakov (Apr 18, 2022 14:38 PDT)</a> Adobe Acrobat Sign Transaction Number: CBJCHBCAABAIRD5q7eTRfLBubPAIL11efeDTyujTftb

\*Add more approval rows as needed.

## Attachment A: Privacy Officer Appointment

In accordance with this policy, Chris Haudenschild is appointed as the Privacy Officer for CliniComp, Intl.

---

Chris Haudenschild

CEO

---

Date

## Attachment B: De-identification of CIS PHI


The de-identification procedure for CIS PHI requires the removal of the following identifiers of the patient or of the patient's relatives, employers, or household members per Title 45 CFR Part 164.514:

- Names
- All elements of a street address, city, county, precinct, zip code, and their equivalent geocodes
- All elements of dates (except year) for dates directly related to the individual (e.g., birth date, admission/discharge dates, date of death), and all elements of dates (including year) that indicate age 89, except that such ages and elements may be aggregated into a single category of age 90 or older
- Telephone numbers
- Fax numbers
- E-mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- License plate numbers, vehicle identifiers and serial numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full-face photographic images and comparable images
- Any other unique identifying number, characteristic or code, except as created by Health Information Systems to re-identify the information, subject to the limitations specified in HIPAA regulation 42 CFR § 164.524(c)

The remaining information must not alone or in combination allow for identification of the patient.

## Attachment C: Transmittal Sheet

Use T039 CliniComp Transmittal Sheet Template, which is located under Regulatory > Templates in SharePoint.

*CliniComp, Intl. Confidential & Proprietary*

### TRANSMITTAL SHEET

TO	<input type="text" value="Type Name here"/>	TOTAL PAGES	<input type="checkbox"/>
COMPANY	<input type="text" value="Type Company Name Here"/>	FAX	<input type="checkbox"/>
FAX NO.	<input type="text" value="Type Fax Number Here"/>	BY HAND	<input type="checkbox"/>
ADDRESS	<input type="text" value="Type Address Here"/>	MESSENGER	<input type="checkbox"/>
ADDRESS	<input type="text"/>	OVERNIGHT	<input type="checkbox"/>
(cont)		U.S. MAIL	<input type="checkbox"/>
PROJECT	<input type="text" value="Type Project Here"/>		
REFERENCE NO.	<input type="text" value="Type Reference No. Here"/>		
FROM	<input type="text" value="Type From Here"/>		
EMAIL	<input type="text" value="Type Email Here"/>		
DATE	<input type="text" value="Type Date Here"/>		

URGENT FOR REVIEW PLEASE COMMENT PLEASE REPLY PLEASE RECYCLE

COMMENTS:

COPY

ENCLOSURE

9655 Towne Center Drive San Diego, CA 92101 +1 (800) 350.8202 | www.clinicomp.com