OH Prescribed Person: Registry of Cardiac and Vascular Services (CorHealth)

The following privacy, security, human resource and organizational Indicators below are provided for Ontario Health (OH) as a Prescribed Person in relation to its Registry of cardiac and vascular services (CorHealth) for the time period of November 1, 2019, to August 2, 2022, unless otherwise specified.

Part 1 – Privacy Indicators

General Privacy Policies, Procedures & Practice

Privacy Indicator	Assessment
Dates privacy policies and procedures were reviewed since prior IPC review	In accordance with the IPC's transfer letter dated December 24, 2021, CorHealth was brought under Ontario Health (OH) as of December 1, 2021. Effective December 2021, CorHealth was subject to the following OH privacy policies and procedures: • OH Privacy Policy • OH Privacy Incident Management Policy and Procedure CorHealth is currently undergoing a transition process to align with all of OH's privacy policies and procedures. Throughout Q1 of the fiscal year 2022/2023 (May and June 2022), an enterprise-wide review of all CorHealth's and OH's privacy policies was conducted to enable the harmonization work underway to integrate with OH. The anticipated date of transition completion and CorHealth's compliance with all of OH's privacy policies and procedures is end of Q3 for fiscal year 2022/2023. During the transition period, and in accordance with IPC requirements, CorHealth continues to maintain compliance with its own privacy policies and procedures. See **Appendix A** for a list of CorHealth's privacy policies and procedures.
Whether amendments were made to existing privacy policies and procedures as a result of the review, and a list and description of each.	Work to harmonize CorHealth and OH privacy policies and procedures is underway and ongoing. OH's Privacy Policies have been updated as necessary to reflect CorHealth's status as a Prescribed Person, including any associated requirements. CorHealth will be subject to all of OH's privacy policies, practices and procedures once harmonization work is complete. Anticipated date of completion is by the end of Q3 for fiscal year 2022/2023.
Whether new privacy policies and procedures were developed and implemented as a result of the review, and description of each	Work to harmonize privacy policies and procedures is underway and ongoing. CorHealth will be subject to all OH privacy policies and procedures once harmonization work is complete. Anticipated date of completion is by the end of Q3 for fiscal year 2022/2023.
Date each amended and newly developed privacy policy and procedure was communicated, and nature of communication	Amended privacy policies were communicated as follows: • Email notification to staff of change and effective date sent November 11, 2021 • CorHealth presentation of change in all-staff meeting November 25, 2021 • Posting of changed policies to intranet December 1, 2021 • Staff signing of agreements/acknowledgements December 1-7, 2021 • OH Privacy training rolled out to staff January 1-31, 2022.
Whether communication materials available to public and other stakeholders were amended as a result of the review, and description of amendments	Communication materials available to the public and other stakeholders (i.e., client brochure, statements of purpose for data holdings, and website updates) were amended to reflect the organization and policy changes during Q1 for fiscal year 2022/2023. Anticipated date of full completion is by the end of Q3 for fiscal year 2022/2023.

Collection

Privacy Indicator	Assessment
Number of data holdings that contain PHI	Data Holdings: 2
Number of statements of purpose for data holdings that contain PHI	Statements of Purpose: 2
Number and list of statements of purpose for data holdings reviewed since the last IPC review	Statements of Purpose Reviewed: 2 • Cardiac Registry: last reviewed May 26, 2022 • Vascular Registry: last reviewed May 26, 2022
Whether amendments were made to existing statements of purpose as a result of the review, and a list of those statements of purpose with a description of amendments made	Since the prior IPC review, CorHealth has reviewed and amended the statements of purpose for both of its PP data assets. Amendments were required to reflect the organizational name change and branding to Ontario Health. See **Appendix B** for CorHealth's Data Holdings and Statements of Purpose List.

Use

Privacy Indicator	Assessment
Number of agents granted approval to access and use PHI for non-research purposes	Total agents granted approval: 61[5] • 47 CorHealth staff members (access to PHI is limited to a subset of CorHealth staff members, as required for their role and in alignment with policies) • 14 service providers
Number of requests received for use of PHI for research since prior IPC review	Total requests received for use of PHI for research: 0
Number of requests for use of PHI for research purposes that were granted and that were denied since prior IPC review.	Request for use of PHI for research granted: 0 Request for use of PHI for research denied: 0

Disclosure

Privacy Indicator	Assessment
Number of requests for disclosure of PHI for non-research purposes since prior IPC review	Requests: 0
Number of requests for disclosure of PHI for non-research purposes that were granted or denied since prior IPC review	Requests denied: 0 Requests granted: 0
Number of requests for disclosure of PHI for research since prior IPC review	Requests: 0
Number of requests for disclosure of PHI for research that were granted or denied since prior IPC review	Total requests granted: 0 Total requests denied: 0
Number of research agreements executed with researchers to whom PHI was disclosed since the prior IPC review	Total agreements: 0
Number of requests for disclosure of de-identified and/or aggregate data for research and other purposes since prior IPC review	Total requests: 44
Number of acknowledgements or agreements executed by persons to whom de-identified and/or aggregate data was disclosed for both research and other purposes since prior IPC review	Total acknowledgements or agreements: 19 19 of the 44 requests for disclosure of aggregate and/or de-identified information were granted and therefore 19 agreements with researchers were executed.

[5] Reduction in the number of Agents since the last IPC review is the result of CorHealth no longer reporting hospital users with access to their own organization's PHI via CorHealth systems as Agents and decommissioning a reporting technology for hospital users to analyze their own data.

Data Sharing Agreements

Privacy Indicator	Assessment
Number of DSAs executed for collection of PHI since prior IPC review	DSAs executed for collection PHI: 0
Number of DSAs executed for disclosure of PHI since prior IPC review	Total DSAs: 2 • Institute for Clinical Evaluative Sciences (ICES), DSA originally executed in June 2016, and amended in May 2017, September 2017, August 2018, June 2019, December 2019, June 2020, and January 2021. • Institute for Clinical Evaluative Sciences (ICES), DSA originally executed in February 2020, and extended in June 2020, and amended in February 2021, March 2021, and November 2021.

Agreements with Third-Party Service Providers

Privacy Indicator	Assessment
Number of agreements executed with third-party service providers with access to PHI since prior IPC review	Total Agreements: 4

Data Linkage

Privacy Indicator	Assessment
Number and list of data linkages of PHI approved since prior IPC review.	Linkages: 0 No data linkages have been approved or implemented since the prior IPC Review.

Privacy Impact Assessments

Privacy Indicator	Assessment
Number of PIAs completed since prior IPC review and for each PIA completed: • Data holding, information system, technology, or program; • Date of completion; • Brief description of each recommendation; • Manner each recommendation was, or is expected to be, addressed. • Date each recommendation was addressed or is expected to be addressed.	Total number of PIAs completed: 1 See **Appendix C** for details.
Number and a list of PIAs undertaken but not completed	Total number: 0
Number and a list of PIAs not undertaken but for which a PIA will be completed and the proposed date of completion	Total number: 0
Number of determinations made that a PIA is not required, and for each the reason	Total number: 0
Number and a list of PIAs reviewed since prior IPC report and brief description of any amendments.	Total number: 0

Privacy Audit Program

Privacy Indicator	Assessment
Dates of audits of agents granted approval to access and use PHI since prior IPC review and for each audit: • A description of each recommendation; • Date each recommendation was addressed or is proposed to be so; and • Manner each recommendation was, or is proposed to be, addressed	Total PHI access audits: 3 Audits of agents who have approval to access and use PHI were completed in conjunction with the annual privacy training campaigns conducted in: • December 2020 • November 2021 • June 2022 No recommendations made as a result of the audits.
Number and list of all other privacy audits since prior IPC review and for each audit: • Description of nature and type of audit; • Completion date; • Description of each recommendation; • Date each recommendation was, or is proposed to be, addressed; • Manner in which each recommendation was, or is proposed to be, addressed.	Total number: 13 See **Appendix D** for details.

Privacy Breaches

Privacy Indicator	Assessment
Number of privacy breaches since prior IPC review	Privacy breaches: 23 Suspected breaches: 0
With respect to each privacy breach or suspected privacy breach: • Date notified; • Extent; • Internal/external; • Nature & extent; • OH (CCO) CEO notified; • Containment; • Containment date; • Third-Party notice; • Investigation start; • Investigation close; • Recommendations; • Implemented	See **Appendix E** for details.

Privacy Complaints

Privacy Indicator	Assessment
Number of privacy complaints since prior IPC review	Complaints: 0
Of the privacy complaints received, the number investigated since prior IPC review and for each the: • Date complaint received; • Nature of complaint; • Date investigation commenced; • Date of letter to individual who complained in relation to the commencement investigation; • Date investigation completed; • Description of each recommendation; • Date each recommendation was, or is proposed to be, addressed; • Manner each recommendation was, or is proposed to be, addressed; and • Date of letter to individual who complained describing nature and findings of investigation and measures taken	Complaints investigated: 0
Of the privacy complaints received, the number not investigated since prior IPC review and for each the: • Date complaint received; • Nature of complaint; and • Date of letter to individual who complained and description of letter's content.	Complaints not investigated: 0

Part 2 – Security Indicators

General Security Policies, Procedures & Practice

Security Indicator	Assessment
Dates security policies and procedures were reviewed since prior IPC review	In accordance with the IPC's transfer letter dated December 24, 2021, CorHealth was brought under OH as of December 1, 2021. CorHealth is currently undergoing a transition process to align with OH security policies and procedures. All of CorHealth's security policies and procedures were reviewed as part this exercise in preparation for harmonization and integration with OH. During the transition period, and in accordance with IPC requirements, CorHealth continues to maintain compliance with its own security policies and procedures in those cases where there will be a transition period to comply with OH security policies and procedures. The anticipated date of transition completion and compliance with all of OH's security policies and procedures is by the end of Q2 for fiscal year 2023/2024. See **Appendix F** for details.
Whether amendments were made to existing security policies and procedures as a result of the review, and a list and description of each	
Whether new security policies and procedures were developed and implemented as a result of the review, and description of each	
Date each amended and newly developed security policy and procedure was communicated, and nature of communication	OH security policies and procedures were communicated to CorHealth staff during OH onboarding and OH security training, completed in December 2021 and January 2022.
Whether communication materials available to public and other stakeholders were amended as a result of the review, and description of amendments	N/A

Physical Security

Security Indicator	Assessment
Dates of audits of agents granted approval to access the premises and locations within them where PHI is retained since the prior IPC review: • Description of each recommendation; • Date recommendation was, or is proposed to be, addressed; • Manner in which recommendation was, or is proposed to be, addressed	Audit was completed on May 27, 2022. Building management provided a list of access cards which was compared against employee list and guest passes. • Recommendation: Complete audit on a quarterly basis moving forward. • Manner to be addressed: Audit requirement was added to quarterly process list and reminder alerts booked.

Security Audit Program

Security Indicator	Assessment
Dates of review of system control and audit logs since prior IPC review and description of findings	The primary component of CorHealth's "Maintenance and Review of Specialized Assessments and System Control and Audit Logs" policy sets out that software provides real-time monitoring of CorHealth data replication and automatically alerts CorHealth IT staff if a technical or security issue with the data duplication arises. Therefore, there is no need to review these system control logs.

Security Indicator	Assessment
Number and list of security audits since prior IPC review and for each: • Description of nature and type of audit; • Date completed; • Description of each recommendation; • Date recommendation was, or is proposed to be, addressed. • Manner in which recommendation was, or is expected to be, addressed	Total Security Audits: 4 See **Appendix G** for details.

Information Security Breaches

Security Indicator	Assessment
Number of notifications of actual or suspected information security breaches since prior IPC review	Number: 0
For each actual or suspected information security breach: • Date of notification; • Extent of actual or suspected breach; • Nature and extent of PHI at issue; • Date senior management notified; • Containment measures; • Date(s) containment measures implemented; • Date(s) notification provided health information custodians or others; • Date investigation commenced; • Date investigation completed; • Description of each recommendation; • Date recommendation was, or is proposed to be, addressed; • Manner in which recommendation was, or is proposed to be, addressed	N/A

Part 3 – Human Resources Indicators

Privacy Training & Awareness

Human Resources Indicator	Assessment
Number of agents who have, and who have not, completed initial privacy orientation since prior IPC review	Total privacy orientations completed: 20 CorHealth staff members completed initial privacy orientation as they either joined the organization or returned from extended leave since the prior IPC review. Total number of CorHealth agents who have not received initial privacy orientation: 0
Date of commencement of employment, contractual or other relationship for agents yet to receive initial privacy orientation and the scheduled orientation date	All CorHealth agents have received privacy orientation.
Number of agents who have, and who have not, attended ongoing privacy training each year since prior IPC review	All active staff members completed the annual privacy training. Any staff member on extended leave at the time was required to complete training upon their return to work. **2020** Annual Training (Dec-Feb): All 31 active CorHealth staff members completed ongoing privacy training. **2021** Annual Training (Nov-Jan): All 34 active CorHealth staff members completed ongoing privacy training. **2022** Annual OH Training for OH Integration (Jan 2022): All 46 active CorHealth staff members completed OH privacy training.
Dates, number and description of privacy communications to agents since prior IPC review	• December 9, 2020 - Privacy and Security Training, Confidentiality, and Non-Disclosure Agreement email • November 25, 2021 - Privacy and Security Training, Confidentiality, and Non-Disclosure Agreement email

Security Training & Awareness

Human Resources Indicator	Assessment
Number of agents who have, and who have not, completed initial security orientation since prior IPC review	Total security orientations completed: 20 CorHealth staff members completed initial security orientation as they either joined the organization or returned from extended leave since the prior IPC review. Total number of CorHealth agents who have not received initial security orientation: 0
Date of commencement of employment, contractual or other relationship for agents yet to receive initial security orientation and the scheduled orientation date	All CorHealth agents have received security orientation.

Human Resources Indicator	Assessment
Number of agents who have, and who have not, attended ongoing security training each year since prior IPC review	All active staff members completed annual security training. Any staff member on extended leave at the time was required to complete training upon their return to work. **2020** Annual Training (Dec-Feb): All 31 active CorHealth staff members completed ongoing security training. **2021** Annual Training (Nov-Jan): All 34 active CorHealth staff members completed ongoing security training. **2022** Annual OH Training for OH Integration (Jan 2022): All 46 active CorHealth staff members completed OH security training.
Dates, number and description of security communications to agents since prior IPC review	• April 27, 2020 - Web Browser Configuration Update to Auto-Update Internet Browsers and Restart your Laptop Daily email. • August 26, 2020 - Ensure your Mobile Device's Operating System (OS) is Up to Date and Restart your Laptop Daily email. • November 27, 2020 - Ensure your Mobile Device's Operating System (OS) is Up to Date and Restart your Laptop Daily email. • December 9, 2020 - Privacy and Security Training, Confidentiality, and Non-Disclosure Agreement email • March 5, 2021 - Ensure your Mobile Device's Operating System (OS) is Up to Date and Restart your Laptop Daily email. • June 10, 2021 - Ensure your Mobile Device's Operating System (OS) is Up to Date and Restart your Laptop Daily email. • September 14, 2021 - Ensure your Mobile Device's Operating System (OS) is Up to Date and Restart your Laptop Daily email. • November 25, 2021 - Privacy and Security Training, Confidentiality, and Non-Disclosure Agreement email. • January 6, 2022 - Ensure your Mobile Device's Operating System (OS) is Up to Date, Restart your Laptop Daily, and Be Aware of Phishing Emails email. • March 24, 2022 - Reporting Phishing Attempts and Junk, Ensure your Mobile Device's Operating System (OS) is Up to Date, and Restart your Laptop Daily email. • July 5, 2022 - Ensure your Mobile Device's Operating System (OS) is Up to Date, Restart your Laptop Daily, and Reporting Phishing Attempts and Junk email.

Confidentiality Agreements

Human Resources Indicator	Assessment
Number of agents who have, and who have not, signed confidentiality agreements each year since prior IPC review	Number of signed confidentiality agreements: • 48 CorHealth staff members • 14 Contractors Number of not signed confidentiality agreements: 0
Date of commencement of employment, contract or other relationship for agents yet to execute confidentiality agreements and date agreement must be	All CorHealth agents have signed the confidentiality agreement.

executed	

Termination or Cessation

Human Resources Indicator	Assessment
Number of notifications from agents since prior IPC review for termination of their employment, contractual or other relationship	Total notifications: • 18 CorHealth staff members resigned. • 3 CorHealth staff members were terminated. • 19 Agents had their contract end.

Part 4 – Organizational Indicators

Risk Management

Organizational Indicator	Assessment
Dates *Corporate Risk Register* was reviewed since prior IPC review	• November 2019 • April 2020 • January 2021 • June 2021 • March 2022 • May 2022
Whether amendments were made to the *Corporate Risk Register* as a result of the review, and description of each.	There were no amendments made to the *Corporate Risk Register* as a result of the reviews.

Business Continuity & Disaster Recovery

Organizational Indicator	Assessment
Dates business continuity and DRP was tested since prior IPC review.	• July 17, 2020 • June 28, 2022
Whether amendments were made to business continuity disaster recovery plan as a result of testing, and description of each.	No amendments were made to the Business Continuity & DRP Policy as a result of the testing. The following amendments were made to the Business Continuity & DRP Procedure as a result of the testing: • Updated CorHealth call tree • Minor formatting, grammatical errors, and references • Policy recommendations have been logged for consideration as part of the policy harmonization with Ontario Health

Appendix A – Privacy Policy and Procedures List

	CorHealth Privacy Policy or Procedure Document	Equivalent OH Privacy Policy or Procedure Document	Compliant with OH Privacy Policy or Procedure Document (Y/N); If "No", expected date of compliance
1.	Annual Review of Privacy and Security Policies and Procedure	Privacy Policy	Y
		Privacy Compliance and Audit Policy	N – Anticipated date of compliance is end of Q3 FY 2023/2024
2.	Transparency of Privacy and Security Policies and Procedures	Transparency Policy	Y
3.	Statements of Purpose for Data Holdings Containing Personal Health Information	Statement of Purpose for Data Holdings Containing PHI Procedure • The OH policy is currently under review with the IPC. Once finalized CorHealth will be required to follow this policy.	Y
4.	Limiting Agent Access to and Use of Personal Health Information	Privacy Use and Disclosure Policy. • Further updates are being incorporated at this time.	Y
5.	Disclosure of Aggregate and/or De-Identified Personal Health Information to Researchers	Privacy Use and Disclosure Policy • Further updates are being incorporated at this time.	Y
6.	Policy and Procedures for the Execution of Agreement with Third-Party Service Providers with Respect of Personal Health Information	Policy for Tracking Agreements with Third Party Service Providers	Y
7.	Aggregation and De-Identification of Record Level Data	Data De-Identification Guidelines	Y
8.	Policy and Procedures for Privacy and Security Auditing	Privacy Audit and Compliance Policy	N – Anticipated date of compliance is end of Q3 FY 2023/2024
9.	Information Security and Privacy Breach Management	Privacy Incident Management Policy and Procedure	Y
		Information Security Incident Management Standard	Y
10.	Privacy Inquiries and Complaints	Privacy Inquiries and Complaints Policy and Procedure	Y
11.	Privacy Impact Assessments	PIA Standard	Y

Appendix B – Data Asset & Statement of Purpose List

	Name of Data Holding	Statement of Purpose	PHI in the Data Holding	Need for PHI	Source of PHI
1.	CorHealth Cardiac Registry	Ontario Health maintains the CorHealth Cardiac Registry of adult patients who undergo certain advanced cardiac procedures for the purposes of maintaining the waitlist and providing advice to the government for strategic planning. Cardiac procedures include, but are not limited to the following: • cardiac catheterization; • percutaneous coronary intervention (PCI); • cardiac surgery including coronary artery bypass graft surgery (CABG) and valve surgeries; • transcatheter aortic valve implantation (TAVI); and • procedures related to regulating or assessing heart rhythm including ablations, electrophysiology studies, and procedures relating to certain devices such as implantable cardioverter-defibrillators (ICDs).	• Demographic data • Health service data • Wait time data • Facility data • Healthcare provider data	PHI is required to monitor wait times across the province to support Ontario's wait time strategy, decisions on funding and staffing, and other activities related to the provision of cardiac care within Ontario.	• Participating Ontario advanced cardiac centres (hospitals) • Ministry of Health
2.	CorHealth Vascular Registry	Ontario Health maintains the CorHealth Vascular Registry of adult patients who undergo certain advanced vascular procedures for the purposes of providing advice to the government for strategic planning. Note: CorHealth Ontario has stopped collection of record-level vascular data containing PHI. However, it maintains the registry to support reporting and strategic planning.	• Demographic data • Health service data • Wait time data • Facility data • Healthcare provider data	PHI is required to support planning, decisions on funding and staffing, and other activities related to the provision of vascular care within Ontario.	• Participating Ontario vascular centres (hospitals) • Ministry of Health

Appendix C – Privacy Impact Assessment (PIA)

	Data holding, information system, technology, or program	Date the PIA was completed	Agent(s) responsible for completing the PIA	Recommendation(s) and the Manner in which each Recommendation was or is expected to be addressed		Date that each Recommendation was or is expected to be addressed
1.	Privacy Impact Assessment & Risk Mitigation Plan for Registry Upgrade Project Transition to Data Collection Information System (DCIS)	30-Nov-2020	CorHealth Privacy Officer	High Risks	1. Incomplete CorHealth privacy policy updates. Risk of confusion and non-compliance with policies. Addressed through ongoing policy harmonization work and OH privacy training as part of organizational integration.	Jun-2022
					2. Operational Agreements with service provider not executed. Risk of non-compliance with privacy policies. Addressed through execution of agreements and agent privacy training. Note: service provider did not have access to PHI prior to execution of agreements.	Dec-2020
					3. Master Service Agreement and Service Order with service provider were not executed. Risk that technical safeguards not implemented. Addressed through execution of agreements and completion of third-party threat and risk assessment (TRA) of security safeguards to ensure implementation.	Dec-2020, Mar-2021, Sept-2021
					4. Master Service Agreement and Service Order with service provider were not executed. Risk that information security safeguards not identified/implemented. Addressed through execution of agreements and completion of third-party TRA of security safeguards to ensure implementation.	Dec-2020, Mar-2021, Sept-2021
				Medium Risks	1. Lack of data governance structure. Risk of interfaces and features in the system being non-compliant with CorHealth's regulatory authority. Addressed through CorHealth's Privacy Officer leading system implementation, and the use of CorHealth's Leadership Team's (CLT's) overarching governance structure, of which the Privacy Officer is a member.	Dec-2020
					2. Update participation agreements with HICs to indicate CorHealth is a PHIPA service provider for sharing and retrieval of records from OH. Addressed through CorHealth integration with OH.	Dec-2020
					3. Risk that administrative safeguards with service provider may not be sufficient to meet requirements for CorHealth Agents. Addressed through terms and conditions in the executed service provider agreements, and Agent privacy training.	Dec-2020
					4. Risk that physical safeguards with service provider may not be sufficient to meet CorHealth requirements. Addressed through terms and conditions in executed service provider agreements, and third-party TRA of security safeguards.	Dec-2020, Mar-2021, Sept-2021
					5. Risk that CorHealth is not transparent regarding its use of cloud infrastructure. Cloud infrastructure for CorHealth system is not yet in production. CorHealth website material has been updated and will be made available through CorHealth's website when the system is in production.	Expected completion by 31-Mar-2023
				Low Risks	1. Agreement related to the electronic master patient index between CorHealth, and the Ministry was not reviewed as part of this PIA. Accepted/closed with no changes to the agreement or scope.	Dec-2020
					2. Ensure access limitations by class of HIC user appropriate to the role. Addressed through user role groups and access permissions developed in the system (underway, but not complete at time of assessment). HICs are also accountable to identify and authorize role assignment for access to their respective data.	Mar-2021
					3. Risk the policy addressing Agent access to PHI does not contemplate information CorHealth has committed to providing to patients. Addressed through policy harmonization efforts and training with OH as part of the organizational integration.	Jun-2022

Appendix D – Privacy Audit Log

	Nature & Type of the Privacy Audit Conducted	Date that the Privacy Audit was Completed	Agent(s) responsible for completing the Privacy Audit	Recommendations arising from the Privacy Audit	Agent(s) responsible for addressing each Recommendation	Date that each Recommendation was or is expected to be addressed	The manner in which each Recommendation was or is expected to be addressed
1.	PHI Access Audit: Review of users granted access to PHI	Dec-20	Service Management Team	Users who no longer require access to PHI should have their access revoked.	IT Operations & Service Management Team	Jan-20	Users no longer requiring access to PHI had their access revoked.
2.	Confidentiality and Non-Disclosure Agreements Audit: ensure CorHealth Agents have signed the Confidentiality and Non-Disclosure Agreements in compliance with policy.	Dec-20	Service Management Team	None.	N/A	N/A	N/A
3.	Privacy Training Audit: ensure CorHealth Agents have completed Privacy & Security Training in compliance with policy.	Dec-20	Service Management Team	None.	N/A	N/A	N/A
4.	PHI Small Cell Suppression: Review CorHealth information products for compliance with data suppression requirements.	Mar-21	Analytics Team	Establish checklist for small cell suppression to ensure complementary suppression is included and referred results are not able to be derived in CorHealth information products.	Analytics Team	Apr-21	Small cell suppression checklist established and implemented for use in report development
5.	PHI Access Audit: Review of users granted access to PHI	Nov-21	Service Management Team	Users who no longer require access to PHI should have their access revoked.	IT Operations & Service Management Team	Nov-21	Users no longer requiring access to PHI had their access revoked.
6.	Confidentiality and Non-Disclosure Agreements Audit: ensure CorHealth Agents have signed the Confidentiality and Non-Disclosure Agreements in compliance with policy.	Nov-21	Service Management Team	None.	N/A	N/A	N/A
7.	Privacy Training Audit: ensure CorHealth Agents have completed Privacy & Security Training in compliance with policy.	Nov-21	Service Management Team	None.	N/A	N/A	N/A
8.	Confidentiality and Non-Disclosure Agreements Audit: ensure CorHealth Agents have signed the Confidentiality and Non-Disclosure Agreements in compliance with policy.	Jan-22	Service Management Team	None.	N/A	N/A	N/A
9.	Privacy Training Audit: ensure CorHealth Agents have completed Privacy & Security Training in compliance with policy.	Jan-22	Service Management Team	None.	N/A	N/A	N/A
10.	Statement of Purpose Audit: ensure CorHealth data holdings containing personal health information have current and accurate statements of purpose	May-22	CorHealth Privacy Officer	Update the statements of purpose to reflect organizational changes and branding.	CorHealth Privacy Officer	Jul-22	Statements of purpose updated and posted to the CorHealth website.
11.	Website Audit: ensure information about CorHealth's privacy and security program provided to the public is comprehensive, updated, and accurate	May-22	CorHealth Privacy Officer	Update CorHealth website content for contact information to reflect Ontario Health CPO and address, update the privacy brochure to reflect organizational changes and branding as well as reference to cloud system use per PIA recommendation.	CorHealth Privacy Officer	Jul-22	Content updated and posted to the CorHealth website.
12.	PHI Access Audit: Review of users granted access to PHI	Jun-22	Service Management Team	Users who no longer require access to PHI should have their access revoked.	IT Operations & Service Management Team	Jun-22	Users no longer requiring access to PHI had their access revoked.
13.	Audit unauthorized storage of PHI: ensure PHI is not being stored on CorHealth's shared hard drive	Jul-22	CorHealth Privacy Officer	None.	CorHealth Privacy Officer	Jul-22	N/A

Appendix E – Privacy Breach Log

	Date Breach was Identified or Suspected	Internal / External	Nature of PHI	Breach Description	Date of Containment	Containment Measure	Date Notification Provided	Date Investigation Completed	Agent to Conduct Investigation	Policy Breach, Privacy Breach, or Suspected Breach	Breach Type	Recommendations	Manner That Recommendations Were Addressed
1.	7-Apr-2020	External	Email to Service Desk included PHI	Email received by Service Desk from cardiac patient relative which included the name of the requestor's family member and medical history. Email forwarded to multiple members of CorHealth team to support request.	8-Apr-2020	Email deleted and ticket in JIRA project also deleted. Requestor informed in new ticket of measures taken to remove PHI. CorHealth team members informed to delete emails containing PHI.	8-Apr-2020	8-Apr-2020	Specialist, Client Services	Privacy Breach	Passive	No further recommendations required as corrective action taken as part of containment measures.	N/A
2.	11-May-2020	External	Email to Service Desk included PHI	Email received by Service Desk from WTIS user included a patient name and medical record number.	11-May-2020	Email deleted and ticket in JIRA project also deleted. Requestor informed in new ticket of measures taken to remove PHI. User also reminded not to include PHI in future correspondence.	11-May-2020	11-May-2020	Specialist, Client Services	Privacy Breach	Passive	No further recommendations required as corrective action taken as part of containment measures.	N/A
3.	29-Jun-2020	External	Email to Service Desk included PHI	Email received by Service Desk from WTIS user included a patient name and health card number.	29-Jun-2020	Email deleted and ticket in JIRA project also deleted. Requestor informed in new ticket of measures taken to remove PHI. User also reminded not to include PHI in future correspondence.	29-Jun-2020	29-Jun-2020	Specialist, Client Services	Privacy Breach	Passive	No further recommendations required as corrective action taken as part of containment measures.	N/A
4.	6-Jul-2020	External	Email to Service Desk included PHI in attachment	Email received to Service Desk from echocardiogram provider included an attachment with PHI included.	6-Jul-2020	Email deleted and ticket in JIRA project also deleted. Requestor informed in new ticket of measures taken to remove PHI.	6-Jul-2020	6-Jul-2020	Specialist, Client Services	Privacy Breach	Passive	No further recommendations required as corrective action taken as part of containment measures.	N/A
5.	9-Oct-2020	External	Email to Service Desk included PHI	Email received to Service Desk from WTIS user included a screenshot with a patient name.	9-Oct-2020	Email deleted and ticket in JIRA project also deleted. Requestor informed in new ticket of measures taken to remove PHI. User also reminded not to include PHI in future correspondence.	9-Oct-2020	9-Oct-2020	Specialist, Client Services	Privacy Breach	Passive	No further recommendations required as corrective action taken as part of containment measures.	N/A
6.	12-Nov-2020	External	Supplemental file included patient characteristic data (aggregated small cell data, not record level PHI)	Small cell data potentially disclosed in a data file accompanying the annual Cardiac Outcomes Report, which included patient characteristics tables with 20-30 cells of aggregated data (including age and age group). Cell counts of less than 5 may be present or may be inferred, which was in contravention of the DSA with data partner.	Jan 7- 29, 2021	Internal staff notified of error. Formal notification provided to data partner. All report recipients requested to delete data file and replace with new file by a specific date. Ongoing monitoring of incident and follow up with report recipients. File destruction confirmed for 151 of the 155 of report recipients.	13-Nov-2020	2-Jan-2021	Senior Vice President, Privacy Officer	Policy Breach	Breach of Agreement	Review procedures/ metrics for calculating small cells. Reporting checklist/procedure to be updated. All relevant staff trained on procedure updates. Ensure all staff have up to date privacy and security training.	Processes reviewed. Reporting checklist/procedure updated. All reporting and data analytics staff trained on procedure updates with scenario-based training. Annual privacy and security training completed.
7.	8-Jan-2021	External	Email to Service Desk included PHI	Email received by Service Desk from cardiac patient relative which included the Name and Date of Birth of requestor's relative.	8-Jan-2021	Email deleted and ticket in JIRA project also deleted. Requestor informed in new ticket of measures taken to remove PHI.	8-Jan-2021	8-Jan-2021	Specialist, Client Services	Privacy Breach	Passive	No further recommendations required as corrective action taken as part of containment measures.	N/A

	Date Breach was Identified or Suspected	Internal / External	Nature of PHI	Breach Description	Date of Containment	Containment Measure	Date Notification Provided	Date Investigation Completed	Agent to Conduct Investigation	Policy Breach, Privacy Breach, or Suspected Breach	Breach Type	Recommendations	Manner That Recommendations Were Addressed
8.	12-Feb-2021	External	Fax to CorHealth included PHI	CorHealth support staff identified a fax sent earlier that included patient name and medical history.	16-Feb-2021	Fax file deleted. Hospital user who sent fax contacted by clinical team.	16-Feb-2021	16-Feb-2021	Specialist, Client Services	Privacy Breach	Passive	No further recommendations required as corrective action taken as part of containment measures.	N/A
9.	11-Mar-2021	External	Email to Service Desk included PHI embedded in picture	Email received by Service Desk from WTIS user included a screenshot with PHI included.	11-Mar-2021	Email deleted and ticket in JIRA project also deleted. Requestor informed in new ticket of measures taken to remove PHI. User also reminded not to include PHI in future correspondence.	11-Mar-2021	11-Mar-2021	Specialist, Client Services	Privacy Breach	Passive	No further recommendations required as corrective action taken as part of containment measures.	N/A
10.	7-Jun-2021	External	Email to Service Desk included PHI in attachment	Email received by Service Desk from WTIS user included an attached report with patient-level data.	7-Jun-2021	Email deleted and ticket in JIRA project also deleted. Requestor informed in new ticket of measures taken to remove PHI. User also reminded not to include PHI in future correspondence.	7-Jun-2021	7-Jun-2021	Specialist, Client Services	Privacy Breach	Passive	No further recommendations required as corrective action taken as part of containment measures.	N/A
11.	6-Jul-2021	External	Email to Service Desk included PHI in attachment	Email received by Service Desk from echocardiogram provider included an attachment with PHI included.	6-Jul-2021	Email deleted and ticket in JIRA project also deleted. Requestor informed in new ticket of measures taken to remove PHI.	6-Jul-2021	6-Jul-2021	Specialist, Client Services	Privacy Breach	Passive	No further recommendations required as corrective action taken as part of containment measures.	N/A
12.	15-Jul-2021	External	Email to Service Desk included PHI in attachment	Email received by Service Desk from WTIS user included an attached quarterly report for user's facility with volumes of less than or equal to five.	15-Jul-2021	Email deleted and ticket in JIRA project also deleted. Requestor informed in new ticket of measures taken to remove PHI. User also reminded not to include PHI in future correspondence.	15-Jul-2021	15-Jul-2021	Specialist, Client Services	Privacy Breach	Passive	No further recommendations required as corrective action taken as part of containment measures.	N/A
13.	27-Jul-2021	External	Fax to CorHealth included PHI	CorHealth support staff identified a fax that included patient name and medical history.	27-Jul-2021	Fax file deleted. Hospital user who sent fax contacted by clinical team.	27-Jul-2021	27-Jul-2021	Specialist, Client Services	Privacy Breach	Passive	No further recommendations required as corrective action taken as part of containment measures.	N/A
14.	14-Dec-2021	Internal	PHI files included patient name, date of birth, health card number, medical record number, patient procedure and patient health related information	Zipped files containing PHI were incorrectly saved to an unauthorized PHI zone in CorHealth's Azure subscription, and to a user/technical resource's laptop, as part of the transfer process from CorHealth to Ontario Health.	14-Dec-2021	All files were deleted from the temporary drive on Azure server and from user's laptop.	14-Dec-2021	15-Dec-2021	CorHealth Privacy Officer	Privacy Breach	Unsecure data transfer	File transfers will be checked by 2 resources to ensure correct content and ensure the transfer files do not contain PHI data.	User reminded of process for secure transfer of PHI, and that destination environment must be authorized for storage of PHI. Administrative safeguards updated to include a second participant for validation when files are being transferred across locations.
15.	22-Dec-2021	External	Email to Service Desk included PHI in attachment	Email received by Service Desk from WTIS user included an attached report with a month of user's facility patient-level data.	22-Dec-2021	Email deleted and ticket in JIRA project also deleted. Requestor informed in new ticket of measures taken to remove PHI. User also reminded not to include PHI in future correspondence.	22-Dec-2021	22-Dec-2021	Specialist, Client Services	Privacy Breach	Passive	No further recommendations required as corrective action taken as part of containment measures.	N/A

	Date Breach was Identified or Suspected	Internal / External	Nature of PHI	Breach Description	Date of Containment	Containment Measure	Date Notification Provided	Date Investigation Completed	Agent to Conduct Investigation	Policy Breach, Privacy Breach, or Suspected Breach	Breach Type	Recommendations	Manner That Recommendations Were Addressed
16.	13-Jan-2022	External	Email to Service Desk included PHI in attachment	Email received by Service Desk from WTIS user included screenshots with two patient postal codes and one patient admission and booking date.	13-Jan-2022	Email deleted and ticket in JIRA project also deleted. Requestor informed in new ticket of measures taken to remove PHI. User also reminded not to include PHI in future correspondence.	13-Jan-2022	13-Jan-2022	Specialist, Client Services	Privacy Breach	Passive	No further recommendations required as corrective action taken as part of containment measures.	N/A
17.	2-Feb-2022	External	Email to Service Desk included PHI in attachment	Email received by Service Desk from WTIS user included a report screenshot with 10 patient names, nine MRNs, and 10 procedure dates.	2-Feb-2022	Email deleted and ticket in JIRA project also deleted. Requestor informed in new ticket of measures taken to remove PHI. User also reminded not to include PHI in future correspondence.	2-Feb-2022	2-Feb-2022	Specialist, Client Services	Privacy Breach	Passive	No further recommendations required as corrective action taken as part of containment measures.	N/A
18.	15-Feb-2022	External	Fax to CorHealth included PHI	CorHealth support staff identified a faxed referral form that included patient name, date of birth, health card number and medical information.	15-Feb-2022	Fax file deleted. Hospital user who sent fax contacted.	15-Feb-2022	15-Feb-2022	Coordinator, Client Services	Privacy Breach	Passive	No further recommendations required as corrective action taken as part of containment measures.	N/A
19.	2-Mar-2022	External	Fax to CorHealth included PHI	CorHealth support staff identified a fax that included patient name, date of birth, health card number and medical information.	2-Mar-2022	Fax file deleted. Hospital user who sent fax contacted.	2-Mar-2022	2-Mar-2022	Coordinator, Client Services	Privacy Breach	Passive	No further recommendations required as corrective action taken as part of containment measures.	N/A
20.	3-Mar-2022	External	Email to CorHealth employee included PHI in embedded screenshot	Email received by Service Desk user's work email and then forwarded to Service Desk email from WTIS user included a screenshot with eight patient names.	3-Mar-2022	Email deleted in personal email and Service Desk email and ticket in JIRA project also deleted. Requestor informed in new ticket of measures taken to remove PHI. User also reminded not to include PHI in future correspondence.	3-Mar-2022	3-Mar-2022	Specialist, Client Services	Privacy Breach	Passive	No further recommendations required as corrective action taken as part of containment measures.	N/A
21.	3-May-2022	External	Email to CorHealth employee included PHI	Email received by Service Desk from patient's family member included the patient's name.	3-May-2022	Email deleted and ticket in JIRA project also deleted. Requestor informed in new ticket of measures taken to remove PHI.	3-May-2022	3-May-2022	Specialist, Client Services	Privacy Breach	Passive	No further recommendations required as corrective action taken as part of containment measures.	N/A
22.	6-July-2022	External	Email to CorHealth Service Desk included PHI	Email received by Service Desk from a hospital user asking for assistance with changing a locked entry in the WTIS entry system. User included patient's MRN and cc'd two other hospital employees on the response email. Patient ID number would have been sufficient in the circumstances.	6-July-2022	Email deleted and ticket in JIRA project also deleted. Requestor informed in new ticket of measures taken to remove PHI, and all email recipients asked to delete/purge emails.	6-July-2022	7-July-2022	Specialist, Client Services	Privacy Breach	Passive	No further recommendations required as corrective action taken as part of containment measures.	N/A
23.	27-July-2022	External / Internal	Email to CorHealth employee included PHI	PHI was included in an email sent to CorHealth employee by hospital staff, cc'd to several other hospital staff. PHI included patient name, age, local LHIN, and high-level clinical details. CorHealth employee responded via email and then forwarded internally.	27-July-2022	OH team member sent a new email chain with the external party and noted not to send PHI to CorHealth via email in the future.	3-Aug-2022	3-Aug-2022	Specialist, Client Services Senior Privacy Specialist	Privacy Breach	Passive	Privacy Specialist instructed CorHealth team member to email all OH and hospital email recipients to delete email from their inboxes and deleted items folders and confirm once complete.	All recipients confirmed emails were deleted.

Appendix F – Log of Security Policies

As of the date of this report, Legacy CorHealth is compliant with the following Ontario Health Security documents.

OH Security Policy or Document
Cyber Security Incident Response Process
Information Security Acceptable Use Policy
Information Security Incident Management Standard
Information Security Policy
Information Security Program Governance
Information Security Risk Management Standard
Information Security Software & Systems Standard
Mobile Security Standard

Legacy CorHealth remains compliant with the following legacy CorHealth Security documents during the transition period.

Legacy CorHealth Security Policy or Document
Physical Security
Secure Retention of Personal Health Information
Secure Transfer of Personal Health Information
Destruction of Personal Health Information
Password Policy
Backup and Recovery of Personal Health Information
IT Policy: Email, Internet, and Computing Devices
Patch Management Policy

Appendix G – Log of Security Audits[6]

	Nature & Type of the Security Audit Conducted	Date that the Security Audit was Completed	Agent(s) responsible for completing the Security Audit	Recommendations arising from the Security Audit	Agent(s) responsible for addressing each Recommendation	The date that each recommendation was addressed or is proposed to be addressed	The manner in which each recommendation was addressed or is expected to be addressed
1.	Threat Risk Assessment: Data Collection Information System	March 2021	CorHealth Privacy Officer	Procedural and ongoing operations improvements	IT Service Management and Development Team	Q4 2022	The DCIS has been decommissioned from the environment assessed in this TRA, the findings are no longer relevant.
2.	Threat Risk Assessment: Data Collection Information System	October 2021	CorHealth Privacy Officer	Procedural and ongoing operations improvements	IT Service Management and Development Team	Q4 2022	The DCIS has been decommissioned from the environment assessed in this TRA, the findings are no longer relevant.
				Address critical and high vulnerabilities from vulnerability assessment		Q4 2022	The DCIS has been decommissioned from the environment assessed in this TRA, the findings are no longer relevant.
				Address medium vulnerabilities from vulnerability assessment		Q4 2022	The DCIS has been decommissioned from the environment assessed in this TRA, the findings are no longer relevant.
				Software development improvements	Development Team	Q4 2022	The DCIS has been decommissioned from the environment assessed in this TRA, the findings are no longer relevant.
3.	Threat Risk Assessment: CorHealth Infrastructure	October 2021	CorHealth Privacy Officer	Procedural and ongoing operations improvements • Increase segregation of duties between system administrators and IT security functions • Accelerate IT system decommissioning schedule	IT Service Management and Development Team	Q1-Q2 FY 2023/2024	Decommission legacy IT systems at CorHealth and transition remaining systems to managed services model of support with clear roles/ responsibilities and related system access between resources.
				Address critical and high vulnerabilities from vulnerability assessment • Strengthen system patching • Increase frequency of vulnerability scans		Q1-Q2 FY 2023/2024	Decommission legacy IT systems and apply OH policies/procedures related to IT operations and security to remaining systems.
				Address medium vulnerabilities from vulnerability assessment • Strengthen security awareness training e.g., social engineering and spear phishing • Establish a cyber security framework		Q1-Q2 FY 2023/2024	Decommission legacy IT systems and apply OH cyber security framework to remaining systems. All staff completed OH privacy and security training, including advanced security training related to social engineering and phishing in Q1-Q2 2023.
4.	Current State Security Health Check & Gap Analysis As part of OH's Cyber Defense Work Stream, a *Current State Security Health Check & Gap Analysis* was performed in Q4 of FY2021 and completed on March 18, 2022. Security Health Check was used to assess the security posture & capabilities of all OH Business Units in order to determine operational gaps in existing people, processes and technologies and is used to prioritize security initiatives within OH, for other future security assessments such as Threat Risk Assessments.	Q1/Q2 2022	OH Information Security Office (OH ISO), with support from CorHealth's Information Security Team	Recommendations are in the process of being implemented. • Security control gaps between OH and CorHealth were identified in the Gap Analysis, following CorHealth's merger with OH. Harmonization work is currently underway to address any gaps identified. • OH is working closely with legacy CorHealth to ensure the adaptation and harmonization of all OH Security policies, processes, and technologies. Based on recommendations from the org-wide Security Health Check, these efforts are aimed at ensuring OH security controls (i.e. security incident response, security monitoring, anti-virus, vulnerability scanning, etc.) are consistently applied across all of its legacy Business Units, their applications, and other digital assets, and ensuring a security baseline is established.	OH Information Security Team and legacy CorHealth's Information Security Team	End of Q2 FY 2023/2024	Significant harmonization work is underway to address any security control gaps identified. OH is working closely with legacy CorHealth to ensure the adaptation and harmonization of all OH Security policies, processes, and technologies.

[6] Confidential information has been removed.