HIPAA IT Security Rule, CMIA and PSQIA Risk & Gap Assessment Report For the Hospital Quality Institute

April 15, 2022

Table of Contents

Executive Summary

Cyber Communication has been contracted for a third time at the request of the Hospital Quality Institute's (HQI) President to perform a risk assessment as measured against three statutes: 1) the Health Insurance Portability and Accountability Act Security Rule (HIPAA IT), 2) the California Medical Information Act (CMIA), and 3) the Patient Safety and Quality Improvement Act (PSQIA) as they pertain to information technology (IT) risk. This assessment is being conducted as an independent security assessment (ISA) in order to ensure that the Hospital Quality Improvement Platform (HQIP) and the California Hospital Patient Safety Organization (CHPSO) fulfill their IT risk management requirements, as defined by the HIPAA IT Security Rule and data security best practices. This ISA also assists in the demonstration of the value and feasibility of future IT security enhancements in order to meet the three statutes assessed in this report.

Table 1 below provides an overview and definitions of the various compliance states. The overall improvement in HQI's compliance in this year's ISA over the assessment completed in 2020 was an approximate 27% improvement in closing or reducing security gaps. This improvement shows a considerable investment in HQI's diligence in providing its over 300 hospitals and institutions with a secure way of providing quality improvement in the treatment of their patients.

Table 1 shows a track record of improvement and is a good indicator that HQI has been utilizing previous ISA reports and making significant progress at remediating the security issues discovered in past years. The biggest example of performance improvement is in the remediation of insufficient safeguards. In 2018, there were 13 gaps identified, in 2020 there were seven and in this year's Security Assessment and Gap analysis there was only one. This is the clearest example of a program that is strengthening compliance and by inference, HQI's ability to safeguard client data.

Table 1: Overview and Compliance States Defined

Compliance State	2022 Percent Compliance	2020 Percent Compliance	2018 Percent Compliance	Sufficiency Principles	Visual Indicator for Table #2
No Gap	77%	55.5%	46%	Safeguard requirements are fully met.	
Partial Gap	21%	32%	31%	Safeguard is insufficient but meaningful progress towards compliance has been made.	
Gap	2 %	12.5%	23%	Safeguard is insufficient and more action is needed to remediate this finding.	

Remediation Findings / Security Compliance at A Glance

Table 2 below provides a visual breakdown of the status of HQI's security compliance for the various IT security safeguards as it relates to this ISA's scope of work. The visual breakdown of the compliance state directly maps to the more detailed information that is described in the IT Security Gap Index Table located in Attachment 1.

Table 2: 2022 Security Compliance Dashboard Table

Standards (Std) & Implementation Specifications (IS)		Compliance Status					
		Std (A)	IS-1 (B)	IS-2 (C)	IS-3 (D)	IS-4 (E)	IS-5 (F)
HIPAA Administrative	1. Security Management Process	PG	N	N	N	G	
	2. Assigned Security Responsibility	N					
	3. Workforce Security	N	N	N	N		
	4. Information Access Management	N	N/A	N	N		
	5. Security Awareness and Training	N	N	PG	PG	N	
	6. Security Incident Procedures	PG	PG				
	7. Contingency Plan	N	N	N	N	N	N
	8. Evaluation of Security Procedure	N					
	9. Bus. Assoc. Contracts or Other Arrangements	PG	PG				
Physical	10. Facility Access Controls	N	N	N	N	N	
	11. Workstation Use	N					
	12. Workstation Security	N					
	13. Device and Media Controls	N	PG	N	N	N	
HIPAA Technical	14. Access Control	PG	PG	N	N	N	
	15. Audit Controls	PG					
	16. Integrity Controls	N	N				
	17. Person or Entity Authentication	N					
	18. Transmission Security	N	N	N			
CMIA & PSQIA	19. PSQIA – Disclosure of non-Safe Harbor data	PG					
	20. PSQIA – Data Logically Separated	N					
	21. CMIA – Sensitive Data is Appropriately Encrypted	N					

	G	= Gap	PG	= Partial Gap	N	= No Gap	N/A	= Not Applicable

Guidance for Risk Remediation

The review of the risk assessment results in the IT Security Gap Index Table in Attachment 1 and the guidance provided below will help stratify the safeguard compliance actions into action groups that can be addressed incrementally. As HQI addresses the gaps found in this ISA, high impact items should be addressed first. For example, a safeguard action that has a gap and is rated as having a high impact should be addressed prior to any medium impact safeguards that have partial gaps.

The gaps and their associated safeguard actions should also be evaluated with the second metric provided in Attachment 1, the Cost Estimate, but because the cost differentiator between "High" and "Medium" is only separated by approximately $15,000, it is less of an influence as compared to the potential financial impact of over $25 million for a complete breach of the Otava CHPSO datastore.

Cyber Communication has provided some guidance below based on overall risk and past breach history in the health care industry. This guidance is provided and rank ordered, in our opinion, from the most important to the least important within the impact gaps, but the order of remediation can be affected by ongoing priorities of the California Association of Hospitals and Health Systems (CAHHS) and/or HQI. Additionally, the following guidance should be used in tandem with CHA's security guidance in order to evaluate an initial remediation priority, but HQI's Compliance Committee must ultimately make these decisions based on the resources available and their own risk appetite.

- HQI must initiate stronger technical audit controls for system activity review (ID #5) [1] which needs to be scheduled and not done on an ad hoc basis. Note: this finding is very similar to the findings made in the 2018 and 2020 ISA report.

- An overriding concern is the Otava datastores with its 2.5 million CHPSO records. Many of these concerns raised in past assessments still remain today, for example:

    a) Audit logs are sent to HQI for analysis on a monthly basis by Otava, but they are not reviewed on a routine basis by HQI staff (more information is in IDs #17 and #18).

    b) The Business Associate Agreement (BAA) with Otava does not fully address the security requirements that HQI is culpable to in the agreements that HQI has with its members (ID #29).

    c) Otava is using a TrendMicro tool to provide some log review capability of the HQI systems, but it is not clear what they are looking for and how timely any notification should be to HQI if there is a risk identified.

- Informal security procedures (examples of due diligence) are robust within CHA

[1] All the identification (ID) references provided are found in Attachment 1: Security Rule Gap Index Table.

and HQI, but more formalization and examples of due care (Policies and Procedures) is needed for compliance and assurance to security statutes and to oversight agencies. Additional information can be found in:

a) Security Incident Response (ID #20)

b) Response and Reporting (ID #21)

There are also items in Attachment 1 that are portrayed as having No Gap but are still a requirement of HIPAA and could impact the reputation of HQI overall with customers. These items (such as disaster recovery and business continuity) are technically missing from the HQI's safeguards, but management has made a conscious decision to defer some of these safeguards until a later date. This decision was made because the risk does not warrant the immediate investment as all of HQI's business processes can be deferred for 30 days or more in a major disaster (this is a NIST standard from SP800-34).

Electronic Protected Health Information Assets and Valuation

HQI has a third-party vendor (Otava) supporting such a healthcare asset with over 2.5 million CHPSO records contained in the CHPSO structured query language (SQL) database. The HQIP's SAS (IBM's statistical analysis and data management software) datastore has over 37 million records in total, but all ePHI has been removed by an upstream cloud provider (out of scope). In the event of a breach at HQI or Otava, the potential cost to the providers and ultimately passed on to the business associate (HQI) could easily exceed $25 million2 and potentially risk HQI over $400 million in fines and class action lawsuits3; therefore, with this level of value, the Otava provider's data stores must be treated as a high value asset. Understanding the potential risk to such a valuable asset will make the cost/benefit assessment of safeguards a more straightforward and justifiable evaluation process. The valuation of the Otava cloud asset in the 2020 assessment was over 37 million due to the over-estimation of the ePHI stored (primarily the HQIP data) and the number of affected individuals if there were a breach.

The other asset under consideration in the scope of this ISA is the HQI desktops, laptops and email. Based on discussions with HQI staff, there is no ePHI stored on these devices, although they could potentially have some sensitive information. However, the workload required to take any sensitive information stored on these HQI devices and convert it to something that may become individually identifiable health

[2] Currently the Otava cloud vendor has 2.5 million individuals with their health care or personal information stored, multiplied by $10 (a ***minimal*** valuation due to the extensive health information stored and used by CHPSO at Otava) equals $25 million potential valuation as an asset at a *minimum*.

[3] Customer PII Most Costly: The loss of customer PII was also the most expensive compared to other types of data ($180 per lost or stolen record vs $161 for overall per record average for 2021). https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic Jul 28, 2021

information[4] would be very difficult, if at all possible. Therefore, these assets are valued at approximately $10,000 which is based on trace or incidental sensitive data that may be stored on them. Additionally, this figure includes the reputational impact to HQI and ultimately to the California Hospital Association (CHA) if the data were openly released in a breach (note: the physical laptop or desktop asset value is not considered in any risk calculation).

Remediations / Reasons for Improvement

This ISA determined that of the applicable IT security standards and implementation specification safeguards, a large percentage (77%) were rated as No Gap (i.e., they are fully compliant with the three statutes in the scope of this project). This improvement represents a 20% increase over the 2020 ISA and demonstrates a strong effort from the HQI staff over the last year to close 11 security gaps. Approximately 2% of this report's safeguards were rated as Gap, and 21% of safeguards were rated as Partial Gap with meaningful progress made towards compliance. Improvements include:

- The security management process has improved dramatically with the continued use of the Compliance Committee and the use of the Protected Health Information Data Governance Structure.

- Formality of a risk management administration process with expectations and oversight has been clearly defined (ID #3) in order to provide greater consistency. This has been accomplished with the Compliance Committee and stronger policies and procedures.

- A more formalized and periodic (ID #2) review of activities and potential risks of HQI data stored at Otava has been enacted.

- Better log capture, retention and log review process; however, better consistency of that log review process remains a vulnerability and a negative finding (ID #5).

- A stronger relationship with the cloud provider Otava and better communication of risks and Otava's custodial responsibilities for logging and identifying and reporting malicious activity of the SQL data stored for the CHPSO program. Otava has the same responsibilities for HIPAA IT compliance as a covered entity since the adoption of the Health Information Technology for Economic and Clinical Health (HITECH) Act (2013/2014). Otava's reputation, customer reference ratings, and testimonials are very high and support HQI's choice of this vendor and the responsibility to safeguard member hospitals' health care data.

- The draft HQI Policies and Procedures (P&P) has been updated as a response to the findings in the 2020 ISA and is being finalized. This updated P&P is slated

[4] https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html#:~:text=%E2% 80%9C Individually%20identifiable%20health%20information%E2%80%9D%20is,care%20to%20the %20 individual%2C%20or

for approval and adoption this year and will close many procedural gaps.

- The identification of essential functions (functions that must be recovered in 30 days or less) and their recovery became “No Gap” due to the determination that all functions could be deferred for over 30 days. If certain functions were determined to be essential then HQI must build recovery and continuity plans for them, but because HQI has no essential functions these standards do not apply. It must be mentioned, however, that HQI does have an obligation to maintain their goodwill with their customers and should consider building and testing these plans in order to maintain current goodwill. As business priorities change, HQI should reevaluate the need for contingency planning efforts.

- The PSQIA requirement for Patient Safety Work Products (PSWP) has been changed to “No Gap” as there is only one PSWP each year and it meets the secure disclosure requirements. All other PSWP’s have been converted to webinars where none of the HIPAA 18 identifiers or any other sensitive data is used or exposed.

The High Price Tag of Data Breaches

Between 2009 and 2021, 4,419 healthcare data breaches of 500 or more records have been reported to the HHS’ Office for Civil Rights. Those breaches have resulted in the loss, theft, exposure, or impermissible disclosure of 314,063,186 healthcare records. That equates to more than 94.63% of the 2021 population of the United States. In 2018, healthcare data breaches of 500 or more records were being reported at a rate of around 1 per day. Fast forward 4 years and the rate has doubled. In 2021, an average of 1.95 healthcare data breaches of 500 or more records were reported each day.[5]

A healthcare data breach comes with a hefty price tag—to the tune of $7.13 million on average for 2021.That's up more than 10% from last year, when the average data breach cost healthcare organizations $6.45 million, according to IBM Security’s 2021 data breach cost report. The IBM study found that 80% of these incidents resulted in the exposure of customers' personally identifiable information (PII). Out of all types of data exposed in these breaches, customer PII was also the costliest to businesses.[6]

IBM and Ponemon studies from 2021 found that the average time to identify and contain a breach in this industry was 329 days and the cost per electronic Protected Health Information (ePHI) record in 2020 was $242[7].

[5] https://www.hipaajournal.com/healthcare-data-breach-statistics/

[6] https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic Jul 28, 2021

[7] 2020 studies from IBM and Ponemon (2020 Cost of Data Breach Study) found that healthcare data breach cost an average of $242 per record with full PHI (not data reduced to a limited data set).

Background, Scope & Approach

Background

HQI (consisting of HQIP and CHPSO among other programs) is a small part of the California Association of Hospitals and Health Systems (CAHHS). HQI is contractually and legally required to comply with the HIPAA Security Rule, CMIA and PSQIA statutes. HQI also faces an evolving landscape of changing regulations, business associate requirements, and technologies that are subject to an array of federal and contractual security compliance requirements. Effective and compliant security practices are essential for HQI and their services that support the improvement of the quality of health care delivery through the analysis, dissemination, and archiving of patient safety information for over 300 hospitals nationwide.

Project Scope

The scope of Cyber Communication's ISA for HQI included:

- Identifying the assets of protection as defined by the HIPAA Security Rule (ePHI).
- Focusing on electronic data and information, in use, transit and at rest.
- The physical, administrative, and technical safeguards used to protect ePHI.
- IT security requirements imposed by the CMIA and the PSQIA.
- Conformance to the National Institute of Standards and Technology (NIST) standards for data encryption and destruction.

The assessment embodied in this report only focuses on HQIP's, CHPSO's and Otava's compliance status as measured against the three statutes (HIPAA IT, CMIA, and PSQIA) and the actions required for achieving compliance with them. Key components of this assessment included:

- ✓ Recognizing HQIP's and CHPSO's trading partner responsibilities – HQIP/CHPSO interface with providers who have compliance obligations under HIPAA. This creates a responsibility in HQI and CHPSO to provide an information security environment that assures trading partners that their information is protected and in compliance with HIPAA/CMIA/PSQIA requirements. Failure to provide this security could make trading partners reluctant to share critical business information with HQIP/CHPSO.

- ✓ Focusing on HQIP/CHPSO's health information (ePHI) only – The HIPAA IT Security regulation and indirectly the CMIA and PSQIA statutes focus on safeguarding of sensitive ePHI.

- ✓ The use and disclosure of non-electronic forms of PHI – The CMIA refers to Individually Identifiable Health Information (IIHI) and references the HIPAA Privacy regulation, however HQIP/CHPSO's work products and business output uses limited data sets in their discussions which represents negligible risk to HQI. The disclosure

risk of verbal or written forms of this information was discussed, but it was determined that the focus needs to be exclusively on the electronic version of the data which is the focus of this ISA.

- ✓ Assessing HQIP/CHPSO adherence to HIPAA Security "safeguards" – HIPAA regulations are founded on industry best practices for information security. This ISA analyzes HQIP/CHPSO's performance relative to the safeguards that comprise this standard of information security.

- ✓ Additional NIST review and assessment – HQIP/CHPSO has varied BAA requirements specific to the NIST encryption and disposal standards. This ISA analyzes HQIP/CHPSO's performance relative to the safeguards that comprise effective information security under these two specific NIST standards.

- ✓ Formulating action strategies for safeguard implementation – This qualitative assessment will guide CHPSO in the formulation of strategies to mitigate the gaps identified in this assessment.

The SQL and SAS databases and file server hosted by Otava are included in the scope of this project as well as laptops, desktops, emails, etc. (see Table 3: Systems / Asset Inventory). Other assets that may be included in the narration of this assessment but are out of scope for this project and include: the NextPlane and Arbor Metrix vendors. It is also prudent to discuss verbal conversations of Protected Health Information (PHI) in the "Safe Table" discussions with providers; however, the staff only use deidentified data or limited data sets (data with very limited examples of PHI) in their work products in order to make their point in these Safe Table discussions.

Gap Assessment Approach

Cyber Communication analyzed the security of systems and infrastructures in the CHPSO environment as they relate to the HIPAA IT Security Rule (and CMIA/PSQIA). By utilizing an established questionnaire derived directly from the statutes, standards, and implementation specifications, Cyber Communication performed remote interviews and off-site reviews of policies, procedures and practices employed by HQI. Cyber Communication also performed one on-site visit in order to review the physical safeguard elements required under the HIPAA Security Rule.

The HIPAA standards and implementation specifications were then incorporated into a Security Rule Gap Index Table (Attachment 1) which includes columns describing a compliant state, CHPSO's current status based on interviews and reviews, and if a gap or partial gap exists, the safeguard action required as well as the impact and qualitative cost estimate to mitigate the gap.

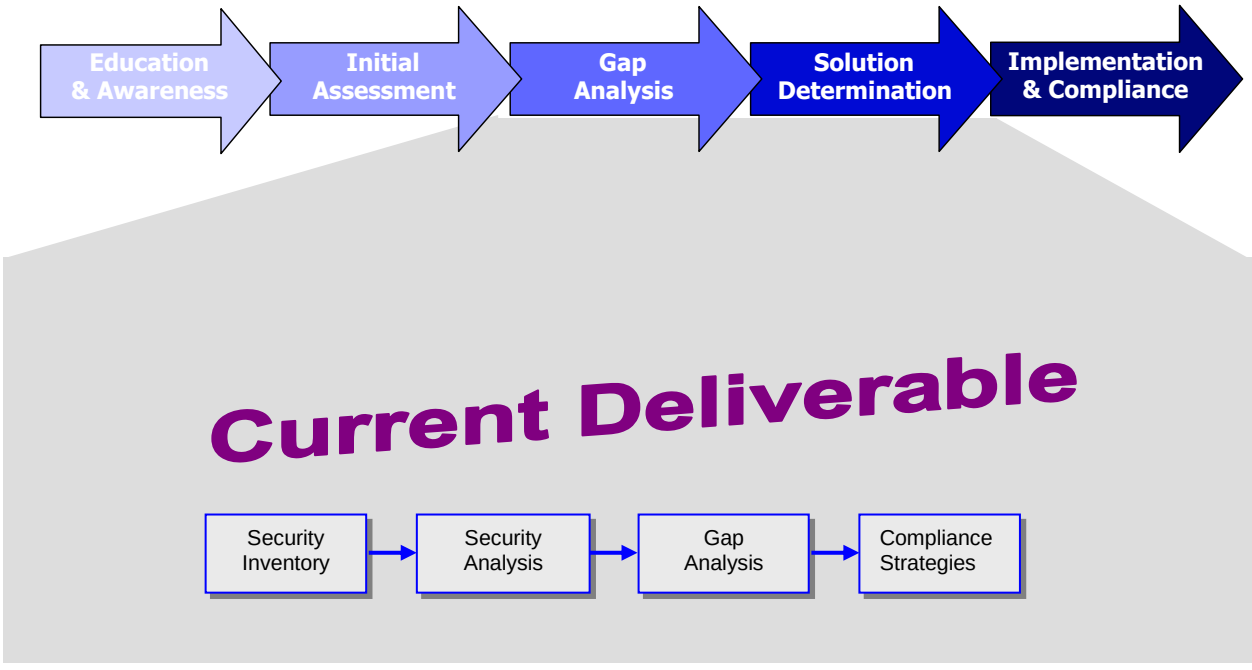
Risk Assessment Approach

This ISA defines a collection of safeguards that must be implemented in order to demonstrate HIPAA/CMIA/PSQIA IT security compliance. The HIPAA regulations recognize that most organizations cannot implement all safeguards simultaneously, since that is often not technically, organizationally, or financially feasible. To address the problem of prioritizing security compliance actions, these statutes point to the use of a risk assessment process as a tool to prioritize HQI's actions. This is a common practice in security management and it is utilized in this ISA.

For this project a qualitative assessment was utilized and included in the Security Rule Gap Index Table. In each standard or implementation specification where a gap or partial gap was determined to exist, an impact level of High, Medium or Low and a similar qualitative cost estimate (High, Medium or Low) was included so that HQIP and CHPSO could prioritize mitigation efforts with an implementation strategy. Additional analysis should be done by HQIP and CHPSO that includes the guidance provided in the Executive Summary and any current risk mitigation projects being done by the parent organization, CHA.

As depicted in Figure 1 below, this project is part of the Risk and Compliance Life Cycle by identifying the gaps and providing guidance to determine appropriate solutions.

Figure 1: Project Steps and the Risk and Compliance Life Cycle



HIPAA Security Inventory

Comprehensive Inventory

The following information assets involve ePHI and support operations at HQIP and CHPSO:

Table 3: ePHI Inventory

Systems/Assets		ePHI Quantity	Owner	HQI Custodian
Otava Cloud Storage		> 2.5 million individuals and their health information (CHPSO)	300+ hospitals	Robert Imhoff
Otava Cloud Storage		Incidental * (HQIP)	300+ hospitals	Robert Imhoff
Laptops		Incidental *	HQIP/CHPSO	Robert Imhoff
Desktops		Incidental *	HQIP/CHPSO	Robert Imhoff
Email		Incidental *	HQIP/CHPSO	Robert Imhoff

* Incidental refers to the possibility that some limited data set or sensitive information may be stored or transmitted against HQI policy.

2020 Security Gap Index Inventory is Referenced

Each cell in the Safeguard and Impact column (the last column) described in the Security Gap Index Table in Attachment 1 has the 2020 assessment score identified. It is provided as a reference to show how and where improvements have been made in the past two years. Attachment 4 has the overview from the 2020 ISA and Attachment 5 has the overview from the 2018 ISA as references.

Attachment 1 - Security Rule Gap Index Table

The table below represents the raw data at a granular level in order to provide specific details on the current state of compliance (HQIP / CHPSO's Current Status). Qualitative (High, Medium, Low) impact and costs[8] as well as suggested actions are included in the final column to assist the HQIP and CHPSO HIPAA Internal Advisory Team to target resources and actions in order to close the identified gaps. The visual overview of the compliance state found in Table 4 below is summarized in Table 2 in the Executive Summary.

Table 4: HQIP and CHPSO IT Security Rule Gap Index

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
1	Security Management Process (Standard 1)	The entity must provide for the protection of its information assets by establishing appropriate administrative, physical and technical policies, standards, and procedures to ensure its operations comply and conform with business requirements, statutes, and administrative policies, and that personnel maintain a standard of due care to prevent misuse. These documents along with a supported enforcement program and active risk management process create the foundation for ongoing security management.	HQI has developed a Protected Health Information Data Governance Structure document that provides guidance to HQI for the Security Management Process and HIPAA. There is a Compliance Committee (November 2021 was the last meeting) that is responsible for setting standards and approving new implementations of security as well as procurements from vendors and remediation of vulnerabilities. HQIP and CHPSO are culpable to HIPAA, CMIA, PSQIA, some NIST standards and various business associate (BA) requirements. Generally, HQI staff performance and activities reflect a high level of awareness of these requirements. Much of the HQIP's data is aggregated and stored in limited data sets in the cloud. CHPSO has a significant amount of ePHI data stored at Otava.	**Partial Gap** – The HQIP and CHPSO programs do seem to have a strong security culture and management process, but continued maturity in oversight of the contracted Otava cloud vendor and a more consistent vulnerability remediation program is needed. Please see report details in the remaining rows of this table. High Impact. High Cost. 2021 = Partial Gap

[8] Qualitative cost estimates include the one-time costs of implementation as well as ongoing annual costs to maintain the process or tool for the foreseeable future. Costs estimates include the variable cost of labor and staff time/effort and are loosely bound by the following criteria:
High would be one-time costs of approximately $30,000 or ongoing costs exceeding $16,000 per year.
Medium would be one-time costs of approximately $15,000 or ongoing costs exceeding $8,000 per year.
Low would be one-time costs of approximately $5,000 or ongoing costs less than $2,000 per year.

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
			CHPSO is the BA of many providers across the country and has a variety of notification requirements described in business associate agreements (BAAs). Otava is governed by a BAA and they are held to the HIPAA standards as a BA, but the BAA does not contain any CMIA or PSQIA language or upcoming privacy language specific to California. HQI has legal counsel available to consult for contract and BAA administrative requirements and CHPSO's (CHPSO is largest PSO) President has an extensive understanding of the diligence required under these various requirements. HQI receives their funding and IT support from the California Hospital Association (CHA). Many technical aspects of the HQIP and CHPSO environments involve IT which is supported by CHA. OTAVA has custodianship of data in the cloud for both HQIP and CHPSO. There are tools available that report on security vulnerabilities, but many logs and reports from these tools are not consistently reviewed. There is a CHA Policy & Procedure document which is the primary policy for all staff and a more specific HIPAA Policy & Procedure document for HQI staff only. There still seems to be some question as to ownership of the data stored at HQI. Some staff says the hospitals retain ownership and HQI's role is only as the custodian.	
2	Risk Analysis Administration (Standard 1, IS-1)	An accurate and thorough risk assessment is conducted and documented to identify potential risks, threats and vulnerabilities to the confidentiality, integrity and availability of all sensitive data held by the entity and approved by management. A thorough risk analysis would consider likelihood and impact of vulnerabilities	This annual assessment and gap analysis report serves as a practical example of risk analysis and administration and measures the compliance to HIPAA Security, CMIA and PSQIA laws and conformance to some NIST standards. Per the CHPSO Security Standards Policy, security assessments shall be performed on an as-needed basis, for example, upon the implementation of a new network or change in physical location. Otherwise, a security review will occur at least annually.	**No Gap** – Note: Per the HQI policy technical vulnerabilities should be reviewed every 6 months. This risk is also covered in ID #17 and #18 in greater detail.

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
		and threats, including losses caused by unauthorized uses and disclosures, as well as loss of data integrity. Program deficiencies are identified through compliance certification reporting, risk assessments, audits, incidents or oversight reviews. This process should be done at least every two years with executive management approving the results.	Periodic phishing exploits are conducted to test staff on their response to such exploits, and reports are provided to CHA (the parent organization of HQIP AND CHPSO). There have been no negative test results from HQI's staff responding to phishing assessments.	2021 = Gap
3	Risk Management Administration (Standard 1, IS-2)	An information security, privacy and risk management strategy is established which includes a clear expression of risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, and a process for consistently evaluating risk across the organization. Security measures are sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level based upon the organization's risk tolerance.	CHPSO has the responsibility of maintaining very sensitive provider data, not only due to the health nature of the data, but also due to the liability of member hospitals in case of a breach of data at HQI. This risk would support a stronger periodic administration of third-party oversight. (Covered in ID #29) The HQI Data Policy has a risk management administration strategy defined, but more due diligence in the application of this strategy needs to be demonstrated. (See ID's #5, #20, and #21) HQIP and CHPSO and its parent organization are very risk averse and have many controls in place to mitigate risk to include Microsoft's Threat protection, email filtering, system logs, enhanced firewall tools, advanced anti-virus tools, etc. These tools are utilized by CHA and provide assurance to technology and data outside the Otava cloud. The Compliance Committee has a strong and formal input into the security at HQI. Currently HQI has $10 million of liability insurance. This coverage could be insufficient where potentially 300+ hospitals and 37 million records are at risk.	**No Gap** 2021 = Gap
4	Sanction Policy (Standard 1, IS-3)	Each entity shall ensure the entity's security policies and procedures are fully documented and entity staff is aware of, has agreed to comply with,	The disciplinary policy does include the wording of termination as a last resort in the disciplinary process.	**No Gap** 2021 = No Gap

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
		and understands the consequences of failure to comply with policies and procedures. The organization employs a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures. Civil penalties are established for wrongful disclosure and unauthorized use of sensitive information. Intentional violation by organization employees is cause for discipline, up to termination.		
5	Information System Activity Review Administration (Standard 1, IS-4)	Procedures are implemented to formalize and regularly review records of information system activity such as audit logs, access reports, and security incident tracking reports. Event logging and log monitoring are performed with sufficient regularity that signs of attack, anomalies, and suspicious or inappropriate activities are identified and acted upon in a timely manner. The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes correlation and analysis of security-related information generated by assessments and monitoring which are communicated to management.	System activity is tracked and logged via Windows Event Log, but neither CHA Information Technology (IT) nor HQI (and CHPSO) actively monitor the logs for exceptions. Otava has logging with daily review for breach events, event notification and a one-year archive is required by HQI (requirement ID# 7600-4706), but this may just be for three devices. The FortiAnalyzer Cloud and vRealize Log Insight tools are used for this process by Otava. Otava sends a log monthly, but HQI only reviews the logged information on an ad hoc basis. HQI keeps an activity log showing when they've reviewed these logs. This process is still not done on a consistent basis. The HQI Data Policy states that "A review of Windows event log data associated with systems hosting protected data must be conducted periodically every six months" but this period is insufficient to reduce risk. PCIDSS standards requires a log review daily and some HIPAA experts refer to this law as an appropriate metric for log review. HQI is reevaluating the six-month review period for their policy. There is notification of major malicious events if a system goes down or if there is a major outage. CHA IT will receive alerts even on weekends from HQI's third-party vendors.	**Gap** – Consistent and periodic system activity review should be performed by CHA IT and/or HQI staff, especially for failed login attempts and large outbound data transfers and account authorization changes (NIST 800-137 may provide some guidance on frequency of monitoring activities). Policy and procedures must provide a framework for consistent system activity review based on the risk appetite of the organization; no specific periodic guidance is provided by the standards within scope of this project. High Impact. Medium Cost. 2021 = Gap

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
			CHA currently has helpdesk FreshService software as their ticketing system. This system does keep a record of helpdesk tickets Per HQI policy, all event log files must be maintained for at least one year. CHA IT uses Microsoft's Advanced Threat Protection to scan social security numbers (SSNs) and medical record numbers (MRNs) and review data saved at Microsoft (Office 365). CHA has never found PHI. Microsoft Defender does have a feature to identify and scan for protected information on SharePoint. Penetration testing by BitSight was done in September 2021 for CHA Cyber Insurance.	
6	Assigned Security Responsibility and Administration (Standard 2)	Identification of a security official who is assigned the authority to develop, issue, and maintain policies, standards, and procedures; direct the organization to effectively manage risk; and advise and consult with the organization's staff and management on security issues. The organization assigns a senior-level executive or manager as the Information Security Officer (ISO) who is responsible for authorizing information systems operation; and ensuring risks are managed before commencing operations.	HQI has assigned Security and Privacy officers. The system administrator performs many of the CHA information security administration functions to include receiving emails from homeland security and Data breach digest alerts and stays current on threats and risks.	**No Gap** 2021 = No Gap
7	Administration of Workforce Security (Standard 3)	Each entity shall safeguard access to information assets by managing the identities of users and devices and controlling access to resources and databases on a need-to-know basis throughout the identity lifecycle. The organization employs the principle of least privilege, allowing only	Each user and process have a unique identifier. Controlling access to resources and data must be authorized by management and the data manager prior to system access. HQI has security language in their policy and CHPSO has more restrictive language involving their work products.	**No Gap** 2021 = No Gap

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
		authorized accesses for users (or processes acting on behalf of users) to information which is necessary to accomplish their assigned tasks in accordance with organizational missions and business functions. Each entity must identify security and privacy roles and responsibilities for all personnel.		
8	Administration, Authorization and/or Supervision (Standard 3, IS-1)	Procedures are implemented for proper authorization and supervision of workforce members with access to PHI. The organization develops, documents, and disseminates to personnel a security policy that addresses purpose, scope, roles, responsibilities, and management commitment to the access of restricted information and privileged functions. These access controls (both physical and technical) are monitored and audited for compliance.	All staff with access to HQIP and CHPSO data sign a confidentiality agreement for access to data; this is only done when they are hired. All staff with access to Patient Safety Work Product (PSWP) must get trained on data security and sign a non-disclosure agreement. Formal procedures are followed to grant access to PHI. CHPSO has a security management policy, but it focuses more on patient safety and providers than CHPSO staff. A BAA covers the safeguards enforced by Otava on their staff. See ID #11 for technical access controls.	**No Gap** 2021 = No Gap

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
9	Workforce Clearance Procedures (Standard 3, IS-2)	Procedures are implemented to determine that a workforce member's level of access is appropriate prior to authorizing access. Workforce members with privileged access must have a need-to-know for that information in the performance of their job, must be appropriately authorized and screened for their access, and must have signed the appropriate documents acknowledging their access responsibilities. Personnel practices must include employment history, fingerprinting, and/or criminal background checks on personnel who work with or have access to confidential, personal, or sensitive information or critical applications.	Human Resources (HR), as part of its hiring process, does a background criminal check and a Department of Motor Vehicle (DMV) check going back seven years. Background checks can include a DMV check depending on driving responsibility. Conflict of interest and confidentiality agreements are part of the onboarding process. HR maintains a checklist and keeps these documents in employee files.	**No Gap** 2021 = No Gap
10	Termination Procedures (Standard 3, IS-3)	Procedures are implemented for terminating access when a workforce member's employment ends, or if the workforce member's access level is determined to be inappropriate. Personnel practices must include termination procedures that ensure organization information assets are not accessible to separated personnel. The organization, upon termination of individual employment, disables information system access within organization-defined time period and terminates/revokes any authenticators/credentials associated with the individual.	Upon termination, CHA's IT changes the individual's account password, physical building access and HQI obtains access to their work files. There is no review of the terminated individual's activity unless it is warranted. HR manages a checklist to ensure that all staff have all required training and HR has a formal process for termination. CHA has a checklist of approximately 30 steps in an offboarding procedures and process, but not a formal policy.	**No Gap** 2021 = No Gap

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
11	Administration of Information Access Management (Standard 4)	The policies and procedures implemented for authorizing access to sensitive information (e.g., ePHI, PII, confidential information) are consistent with the applicable requirements of the HIPAA Privacy and Security Rules, specifically the "minimum necessary" requirements for use and disclosure of PHI. Each entity must identify security and privacy roles and responsibilities for all personnel. The organization employs the principle of least privilege and the separation of duties to minimize the ability of inside management personnel, outside vendors and customers.	Staff have access to the level they need to do their job and no more. Staff have restricted access to the structured query language (SQL) SAS data through the Otava portal in a role-based system. Otava has no direct access to any HQIP and CHPSO server data, but some may be able to gain access as administrators for Otava. HQI has no visibility to how many Otava staff have administrative rights to the HQI data stored in the cloud, but a BAA covers Otava's responsibilities. All files used within HQIP and stored in the Otava cloud (and that are transmitted in/out to/from providers and universities) have very limited data sets with only zip codes, ages and diagnostic codes. It is a violation of HQI policy to store ePHI on desktops or laptops. Controlling access to resources and data must be authorized by management prior to system access.	**No Gap** 2021 = No Gap
12	Isolating Health Care Clearinghouse Functions and Administration (Standard 4, IS-1)	If a health care clearinghouse is part of a larger organization, then policies and procedures are implemented that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. The organization separates organization-defined duties of individuals, documents separation of duties of individuals, and defines information system access authorizations to support separation of duties.	HQIP and CHPSO do not perform any health care clearinghouse functions.	**N/A**

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
13	Administration of Access Authorization (Standard 4, IS-2)	Policies and procedures are implemented for granting access to sensitive data; for example, through access to a workstation, transaction, program, process, or other mechanism that is commensurate with job-related responsibilities. The organization specifies authorized users of the information system, group and role membership; and access authorizations (i.e., privileges) and other attributes (as required) for each account, and individuals requiring access to information assets sign appropriate user agreements prior to being granted access.	All HQI CHPSO staff members must sign a confidentiality agreement that prohibit discussions of PSWP with anyone in the parent organizations or persons without a need-to-know. For HQI only a few people use the cloud. There are two separate environments (CHPSO and HQI). Neither one is Microsoft Active Directory (AD) managed, but CHA IT utilizes role-based access control. All employee access must be authorized by their management and approved by HQI management. The "O:" drive is used as the CHPSO team share drive located in the Otava cloud.	**No Gap** 2021 = No Gap
14	Administration of Access Establishment and Modification (Standard 4, IS-3)	Each entity shall establish processes and procedures to ensure periodic recertification of access control rules to identify those that are no longer needed or provide overly broad access to an individual or asset. The organization creates, enables, modifies, disables, and removes information system accounts in accordance with organization-defined procedures or conditions and such modifications are periodically audited.	System access is defined based on role-based rules and the process is managed by CHA IT through Windows Server Security. During COVID-19, all staff worked from home daily using CHA owned laptops via a Fortinet VPN to Otava. One system administrator uses GoToMyPC to download or upload files from/to their HQI owned desktop or access to the Otava environment through Fortinet. The need for access level is audited by HQI. Multi-factor authentication is used for GoToMyPC remote access Multi-factor authentication is not used for access to the Otava cloud. CHA has no access to the HQI data in the Otava cloud. CHA scans laptops with Malwarebytes and MS Threat Protection.	**No Gap** 2021 = No Gap

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
15	Security Awareness and Training (Standard 5)	A security awareness and training program is provided for all members of the workforce, including management. The training program, which accounts for new hires and level of information access, is an ongoing, evolving process in response to environmental and operational changes affecting the security of sensitive information. Each entity shall establish rules of conduct for persons involved in the design, development, operation, disclosure, or maintenance of records containing personal information and instruct such persons with respect to legal requirements.	All staff must attend KnowB4 security awareness and training when hired. All staff with access to HQIP and CHPSO files receive updated training annually. Staff seem very risk averse. Attendees from outside CHPSO must attend required training before attending "Safe Table" meetings[9]. HQI, HQIP, CHPSO, and CAHHS employees and contractors who have access to PSWP receive training materials prior to first contact with or potential access to PSWP. The onboarding process includes formal security training by KnowB4 and HIPAA specific training. (Note: Cyber Communication staff took the HIPAA awareness training and felt the training was excellent). There are periodic security training and phishing exploits testing the security knowledge of HQI staff. KnowB4 conducts the phishing tests and cyber security safety training. Note: the phishing emails are routinely treated as spam and going directly to employee spam folders. Therefore, staff are not actually being "tested". There is an accounting done by HR of staff who have attended the annual training. Cyber Communication took the KnowB4 training and found it to be complete and of good quality regarding security basics and HIPAA specific information.	**No Gap** 2021 = No Gap

[9] Safe Tables are educational teleconference presentations and are never recorded. In the Safe Table presentations clinical ePHI may be discussed verbally but is typically not part of the slide deck. One set of slides is used during the GoToWebinar meeting. Another slide deck is redacted of logos and anything identifiable and sent to participants after meetings. From 12 to 60 people attend each webinar.

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
16	Security Reminders (Standard 5, IS-1)	Periodic security reminders are provided for workforce members to reinforce the organization's security program objectives. The organization receives security alerts, advisories, and directives from external organizations on an ongoing basis. Internal security alerts, advisories, and directives are generated as deemed necessary.	KnowB4 does repeated annual training, mostly about phishing and social engineering, behavioral protection, and viruses for general security awareness. Periodic phishing testing is ongoing for all staff (unfortunately many of the testing emails are going directly to the employees' spam folder). KnowB4 sends out security reminders once every week.	**No Gap** 2021 = No Gap
17	Administration and Protection from Malicious Software (Standard 5, IS-2)	Procedures are implemented to guard against, detect, and report the presence of malicious software and these are incorporated into the training program. Each entity shall employ malicious code protection mechanisms at information asset entry and exit points and at workstations, servers, and mobile computing devices on the network to detect and eradicate malicious code. Security patches and security upgrade policy should include, but not be limited to, servers, routers, and firewalls. The policy should address application and testing of the patches and/or security upgrades, in addition to departmental criteria for deciding which patches and security upgrades must be applied, and how quickly.	The Patching Matrix v3 (log of patch status maintained by HQI) seems to be a very complete accounting of the software used at HQI. There are numerous examples of best practice, but also some examples where IT is "investigating" a patch/alert strategy and has yet to resolve a process. Windows Server Update Services (WSUS) automatically updates MS applications and systems. Many applications are run from the cloud and are also automatically updated (i.e., Adobe). The BitSight penetration test was done in September 2021 for the CHA environment. Few vulnerabilities for the CHPSO SQL system remain (where the ePHI is located), But multiple vulnerabilities remain on the HQIP SAS system. Per the HQI Data Policy 11012021, a patch schedule is documented, but the approach to patches that cannot be "auto-updated" is vague and not actionable. Patching of network equipment is the responsibility of CHA and it is done automatically by Cisco. Emails from Cisco is automated and alerts staff of malware issues. The network is also automatically updated to the newest revisions. Malwarebytes flags suspicious files and quarantines the file until CHA can do a scan on the file.	**Partial Gap** – The HQIP SAS and CHPSO SQL server needs to be on a routine patching schedule with the process mandated by policy and detailed scheduling based on patch priority defined. Patching responsibilities need to be clearly defined regarding application and operating system (OS) support. The vendor's (Otava) patching must be audited to verify due diligence. It is not clear who and when various other third-party applications (non-OS patching such as Java, Flash, FTP client, Anaconda, "R" and Adobe) are patched and this process seems to be ad hoc or missing completely. Note on frequency of evaluations: NIST Section 3544 requires the "periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually."

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
			The entire IT group at CalHospital.org receives the alerts of malicious activity to the network and some systems. They also receive alerts on the weekend. For the internal systems, IT can remote into the server if needed to remediate technical issues. Otava is the third-party service provider (virtual machines, provisioning, hardware) providing VMWare environment patching and some Microsoft patching. HQI runs the third-party patching requirements for layered software (SQL) and other third-party software products including SAS and SAS tools. Major SAS upgrades are handled by a SAS-preferred vendor, Strong Tower. It appears that no one is actively patching two applications used for SAS data review, "R" and Python (per the Patching Matrix V3 – Note: this environment doesn't contain any ePHI). CHPSO uses Adobe in the cloud as a service. CHA IT is the only team authorized to install or update any application on the HQI workstations. HQI has no privileges to install or update any software on these platforms. CHA IT uses Team Viewer for remote access and troubleshooting on HQI workstations. Every laptop/desktop has Microsoft Advanced Threat Protection (ATP) and Malwarebytes installed. CHA IT is not responsible for the HQI website. Tenup Inc. hosts the site and is responsible for system upgrades. There is no ePHI data or access associated with this website. CHA IT scans the SharePoint system for ePHI data.	Reference is available at http://csrc.nist.gov/drivers/documents/FISMA-final.pdf. High Impact. High Cost. 2021 = Gap

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
			CHA IT monitors the network using Cisco Meraki for the type of traffic and quantity outside the established business norms of traffic. Otava access is through the Fortinet VPN client. HQI is looking into Otava expanding the use of TrendMicro's tools for patch management.	
18	Administration of Log-in Monitoring (Standard 5, IS-3)	Procedures are implemented to monitor login attempts and to report discrepancies. The organization monitors information system accounts for atypical usage and reports atypical usage of information system accounts to organization-defined personnel. Logs stored for future review.	CHA IT is involved in technical security and occasional log monitoring; they also monitor the network traffic through the Meraki networking gear. They receive alerts and notifications of malicious activity or unauthorized logins. Syslog's default log location is on the same server as the data that it is monitoring. The need for access level to sensitive data is periodically audited by HQI. Technical logical controls to the SQL data seem to be logged but not proactively reviewed (also see ID #17 and #48). There is a Word document that catalogs the log reviews performed by HQI, but the work is not done on a periodic basis (see ID #5). Microsoft's ATP sends alerts that are routinely reviewed by CHA IT. CHA IT does have backup staff if the primary is not available to review log data.	**Partial Gap –** All logs should be routinely monitored for malicious activity and failed login attempts. This activity is ad hoc for access to systems hosted by Otava, although a file is downloaded to HQI on a monthly basis. Threat shared with ID #48 and #5 High Impact. Medium Cost. 2021 = Partial Gap
19	Administration of Password Management (Standard 5, IS-4)	Procedures are implemented for the creation, changing, and safeguarding of passwords. Passwords must be of sufficient strength to safeguard information assets based on organization-defined risk. Privileged accounts must use stronger authentication mechanisms	Password length on the desktop and in the cloud is 14-characters or more at HQI. CHA IT enforces a 12-character password with multi-factor authentication (MS authenticator is used for cell phones as the second dual factor. CHA has initiated Azure Multifactor authentication for access to Azure.	**No Gap** 2021 = Partial Gap

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
		such as multifactor mechanisms to authenticate users and devices The organization must ensure that changing/refreshing authenticators is sufficiently frequent to protect the information from unauthorized access, use, disclosure or modification.	Staff are required to enter a secondary password to access the Otava environment (they need their primary password to access their HQI computer) and this access is also dual-factor. Some passwords are set "not to expire," but general users are set to expire in 360 days. Domain administrator for the local network has stronger access requirements. NIST's Special Publication 800-63B would be more restrictive than Microsoft's password guidance being practiced at HQI. There are no shared accounts, each user has a unique login. A Privileged Access Management (PAM) solution (from Thycotic) is installed at the cloud vendor and requires dual factor authentication per policy and practice.	
20	Security Incident Procedures (Standard 6)	Policies and procedures are implemented to detect and correct the attempted or successful unauthorized use, disclosure, modification, or destruction of information, or interference with system operations. Each entity shall implement incident handling for information security and privacy incidents that includes preparation, detection and analysis, containment, eradication, and recovery.	There is a documented incident response policy, but no documented Incident Response Plan. There is no formal incident handling procedure, but ad hoc procedures are practiced and notification does meet most due diligence practices. The helpdesk ticket system does track some events for historical reference; CHA IT manages the IT helpdesk. Event management is done at both the Otava and CHA side which can add some complexity if not detailed in incident management procedures.	**Partial Gap** – Incident procedures should be formalized in a procedure with triggers and escalation steps. Medium Impact. Medium Cost. 2021 = Partial Gap
21	Response and Reporting Administration (Standard 6, IS-1)	Policies and procedures are implemented so that suspected or known security incidents are identified and, to the extent practicable, harmful effects of security incidents are mitigated. All security incidents, and the outcome of their investigation, are documented and periodically reviewed	Per HQI policy the CHA IT team is responsible for monitoring inside HQI and the protected data cloud vendor (Otava) is responsible for monitoring in their environment; this policy is supported by the BAA. There is no BAA with CHA, but per management there is no requirement as HQI is part of CHA.	**Partial Gap** – The process should be formalized in a policy and procedure. Note: the member hospitals and some third-party vendors were out of scope for this project. Some of HQI's BAs (providers) are located out of state and may have vastly different breach and

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
		as part of the ongoing risk management process. Every organization must promptly investigate incidents involving loss, theft, damage, misuse of information assets, or improper dissemination of information. Additionally, any breaches of unencrypted personal information must be reported to the individual or business associate whose information may have been disclosed, acquired or viewed unless the entity can demonstrate that there is a low probability that information involved was compromised or acquired. This requirement also flows down to business associates and third-party vendors of covered entities.	There are reporting mechanisms from various network and security tools actively used by CHA, but no periodic log or incident review by HQI. HQI BA reporting responsibilities (to their providers and hospitals) are kept in a database and notification timelines are followed, although there has not been a breach at HQI or CHPSO to test the informal breach notification process. Otava has monitoring and event notification for three devices per HQI requirements (ID# 7600-4706) (from above ID #5).	reporting requirements; these should be reviewed. Medium Impact. Medium Cost. 2021 = Partial Gap
22	Contingency Plan Procedures (Standard 7)	Policies and procedures are established to protect the availability, integrity, and security of data during emergency or unexpected events. Each entity shall ensure individuals with knowledge about business functions of the organization participate in the business continuity planning process to identify essential missions and business functions and associated contingency requirements.	A disaster recovery policy exists, but not a disaster recovery plan or procedures. In the event of emergency (e.g., computer failure or unavailable IT resources) the President or designee can authorize temporary access for resolving the emergency to a person who is not yet trained. The data integrity responsibility for some of the HQIP and CHPSO ePHI data has been transferred to Otava. Regarding Otava, "In the event of a disaster, DraaS clients will be prioritized over those using Veeam Backup." HQI is a OTBackup customer and as such, not considered to be a business continuity/disaster recovery (BC/DR) customer. There are no time sensitive business functions (30-days or less as per NIST 800-34) at HQIP and CHPSO.	**No Gap** – There are no time sensitive business processes that need recovery by contract. HQI could have some lost goodwill and should create a contingency plan to protect their image. 2021 = Gap

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
			Per HQI policy, a HQI disaster recovery plan (DRP) has been included in a "CHA-level DRP" that can be referred to as a source for some disaster responsibilities. Backup Simple (Commvault software 1) is used for data backup in the MS cloud.	
23	Data Backup Plan Administration (See #42 for data backup physical safeguards) (Standard 7, IS-1)	Procedures are implemented to create and maintain retrievable exact copies of ePHI. Each entity shall perform regularly scheduled backups of system and user-level information. Backups shall be conducted at the operating system, application, and user level. The detailed procedures should include hardware, software (including version), data file back-up and retention schedules, off-site storage details, and appropriate contact and authority designation for personnel to retrieve media. Each entity shall establish an alternate storage site, including the necessary agreements to permit the storage and recovery of backup information.	Per the HQI data policy, backup retention must meet the HIPAA six-year retention requirement. There is a procedure in that policy to save six one-year copies. Deleted or changed data that has been modified in the SQL database does not have any retention period and is not available to HQI after 14 days. This may not be an issue but it should be defined as a practice in the HQI and CHPSO policies and procedures. CHPSO data can be restored from the providers. CHA only retains the local MS cloud data for 18 months, but they are not the covered entity.	**No Gap** 2021 = Partial Gap
24	Administration of the Technology Recovery Plan (Standard 7, IS-2)	Procedures are established to restore any loss of data and provide a recovery strategy that supports the organization's mission critical functions and critical application priorities. Identification and evaluation of alternative recovery strategies are evaluated and presented to management. Each entity shall develop a Technology Recovery Plan (aka, Disaster Recovery	No HQI technology recovery (aka disaster recovery) plan exists (there are some Otava recovery requirements mentioned in policy and capability due to the changed backup strategy using Veeam). HQIP and CHPSO could pull a fresh copy of the data from member hospitals and could use NextPlane/Otava web interface if an issue required access during an interruption or disaster. There are no time sensitive business functions at HQIP and CHPSO, so operations could be down for an excess of 30 days without impact.	**No Gap** – There are no time sensitive business processes that need recovery by contract. HQI could have some lost goodwill and should create a technology recovery plan to protect their image. 2021 = Gap

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
		Plan) in support of the entity's Business Continuity Plan (BCP) and the business need to protect critical information assets to ensure their availability following an interruption or disaster. Each entity must keep its BCP up-to-date.		
25	Administration of Emergency Mode Operation Planning (Standard 7, IS-3)	Procedures are established to enable continuation of critical business processes for protection of the security of ePHI during and immediately after a crisis situation. The organization develops a contingency plan that addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented.	The requirement for the recovery of the HQIP and CHPSO operations could extend past 30 days; therefore, they do not need an emergency operations plan (NIST 800-34 standard). Additionally, SQL data is available from the Otava internet portal and laptops are available to access that data.	**No Gap** Note: there is no business case requirement for emergency mode operations as there are no critical functions that must be recovered within 30 days so there is not any need for an emergency plan. 2021 = No Gap
26	Testing and Revision Procedures (Standard 7, IS-4)	The procedure for periodic testing and revision of the contingency plan is implemented. The result of the testing is reviewed and provides input into the contingency planning process. Each entity shall test the BCP to determine its effectiveness and the entity's readiness to execute the BCP in the event of a disaster. Each entity shall initiate corrective actions and improvements to the BCP based upon deficiencies identified during testing and exercises.	No tabletop exercises to test a contingency plan have been done since a plan does not exist; however, CHA IT has had the opportunity to successfully recover files in the past year. There is currently no ability to test in the Otava environments.	**No Gap** – There are no time sensitive business processes that need recovery by contract. HQI should consider developing a disaster recovery/business continuity plan and perform testing on basic recovery strategies to prevent loss of goodwill. 2021 = Gap
27	Applications and Data Criticality Analysis Procedures (Standard 7, IS-5)	The relative criticality of specific applications and data is evaluated in support of the other components of the contingency plan.	The HQIP and CHPSO systems are all considered low priority in a disaster scenario. HQIP and CHPSO would want the daily processes working within a month, but could tolerate longer if resources were constrained.	**No Gap** – No system meets the mission critical requirement of 30 days or less. 2021 = No Gap

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
		Each entity shall ensure individuals with knowledge about business functions of the organization participate in the business continuity planning process to conduct a business impact assessment to identify critical functions, systems and dependencies, and prioritize their recovery based on necessity. For mission critical systems, the information system implements transaction recovery for systems that are transaction-based.		
28	Evaluation of Security Procedures (Standard 8)	An evaluation of security controls and safeguards is conducted periodically, or as new technologies are implemented or in response to newly identified risks. This evaluation process may be conducted internally or by an external accreditation agency. Each entity shall validate compliance with all information security policies, standards, and procedures as set forth in requirements as dictated by the entities legal department and internal information security policies to verify that security measures are in place and functioning as intended. Each entity's validation processes shall include ongoing assessments of key security measures and controls in both in-house and outsourced systems.	Policies come from a Compliance Committee. The HQI data policy states that HIPAA audits will be done annually unless minimal change has occurred. A technical vulnerability assessment was done in December 2021 and remediation efforts are underway. CHA IT performs some internal security evaluation/audit functions and a network scan was produced in 2021. All the CHA findings have been remediated. Any device used to access HQI data in the cloud is provided by CHA IT and must conform to their standards. The last Otava SOC 2 was performed in July 2021 and a self-certified "bridge letter" states that controls have not changed since (letter dated 3/1/2022). This does meet the requirement of an independent evaluation. This Cyber Communication HIPAA risk assessment is an example of an ongoing evaluation of administrative, technical and physical security controls. Per CHA, a verification of successful software update deployments are performed by the software "FreshService".	**No Gap** – 2021 = Partial Gap

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
29	Administration of Business Associate Contracts and Other Arrangements (Standard 9)	Appropriate contract language is included with the business associate contracts, memoranda of understanding with other government programs, or other arrangements. These agreements allow a business associate to create, receive, maintain or transmit sensitive information; also, that the business associate has provided assurance that appropriate safeguards are in place to protect the information. Each entity acting as a business associate or operating under a memorandum of understanding shall ensure compliance to the agreements and with applicable statutes, Executive Orders, directives, policies, regulations, standards, and guidance.	The Microsoft SQL and SAS datastores are where HQIP and CHPSO's ePHI data is stored at Otava. This data storage is governed by a BAA. A great deal of risk is transferred to Otava. A review and an assurance of security measures were validated by SOC 2 reports and a "bridge letter" attested to the current level of security measures at Otava. All regulatory requirements should be pushed to HQI vendors through the use of a BAA. Some of these requirements are missing in the current BAA boilerplate document and in the Otava BAA (CMIA and PSQIA). Per the HQI data policy, BAA risk reviews are included in an annual review process as required by the Compliance Committee, but this has not consistently been done. HQIP and CHPSO act as a BA to multiple providers and other entities. HQI has a "boilerplate" BAA that they send to providers who use CHPSO as their PSO. This BAA was revised a "few years ago" to include HITECH language, but has not been reviewed recently. HQI's BAA does not have any CMIA language in it.	**Partial Gap** –BAA language must include the requirements for the CMIA law. Upcoming (2022/2023) California privacy requirements must be included in future BAA contracts. Medium Impact. Medium Cost. 2021 = Partial Gap

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
30	Administration of Written Contracts or Other Arrangements (Standard 9, IS-1)	The business associate contract (or other arrangement) documents the assurances by the business associate that appropriate administrative, technical, and physical safeguards are in place to protect ePHI. Entities are required to enter into written agreements with other entities when they engage such entities in the development, use, or maintenance of information systems, products, solutions, or services.	CAHHS (CHA) employment job descriptions have not been reviewed for a few years; all security requirements should be clearly defined and maintained in these internal documents. Future laws will include the California Privacy Rights Act (CPRA). The California law governing the handling of California residents' personal information. This dramatic expansion of employers' data obligations will go into effect on January 1, 2023, and will require significant changes to existing policies, procedures, and practices for handling individuals' personal information. (CPRA is out of scope for this assessment).	**Partial Gap** – A periodic review of all service agreement requirements requiring attestation (HIPAA, CMIA, PSQIA) should be reviewed annually or as prescribed by the HQI Compliance Committee, especially to/from third-party vendors to ensure compliance with statutes. Note: this standard is not calling out the BAA requirements found in ID #29. Medium Impact. Low Cost. 2021 = Partial Gap
31	Physical Facility Access Controls (Standard 10)	Policies and procedures are implemented to limit physical access to facilities while ensuring that properly authorized access is allowed. Physical security and environmental controls shall include management and maintenance of facility entry controls and badging systems for personnel and visitors. The organization enforces physical access authorizations at entry/exit points to the facility where the information system resides by verifying individual access authorizations before granting access to the facility. Ingress/egress to the facility is controlled using physical access control systems/devices.	Cardkey access and validation is required at all times for HQI office space and the server room. CHA IT manages the cardkey system and backs up the data periodically. Some staff have 24-hour access. All staff use access cards during the day. As well, all staff need cardkey access to the elevators, stairways and doors on weekends and after hours. There is a guard stationed in the lobby of the building during working hours and most external doors are locked. Cyber Communication did a physical on-site review and validated the security protocols and safeguards as sufficient during the 2022 HIPAA security assessment.	**No Gap** 2018 = No Gap

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
32	Physical Contingency of Operations (Standard 10, IS-1)	Procedures are established that allow facility access in support of data restoration activities as a component of the disaster recovery and continuity plans in the event of an emergency. The organization establishes an alternate processing site including necessary agreements to permit the transfer and resumption of information system operations for essential mission/business functions when the primary processing capabilities are unavailable.	No processes exist, but HQIP and CHPSO would not need the daily processes working for at least a month after a disaster and could tolerate longer outages. There is an Office 365 cloud backup done by CHA IT and stored in the event of a disaster. HQI has been working from home with no impact to the business operations for two years.	**No Gap** – No systems meet the mission critical requirement. 2021 = No Gap
33	Physical Facility Security Plan (Standard 10, IS-2)	Each entity shall establish and implement physical security and environmental policies, procedures and protection controls to safeguard the facility and information assets against unauthorized access, use, disclosure, disruption, modification, theft or destruction.	Building security and equipment room security is sufficient to meet the requirements of HQIP's and CHPSO's environments.	**No Gap** 2021 = No Gap
34	Physical Access Control and Validation Procedures (Standard 10, IS-3)	Procedures are implemented to control and validate a person's access to facilities based on their role or function, to control access to software programs for testing and revision, and to control visitor access to a facility. Each entity shall monitor physical access to information systems to detect and respond to physical security incidents, review physical access logs and, upon occurrence of an incident, coordinate results of reviews and investigations with other entities as needed. The organization develops, approves, and maintains a list of individuals with	Cardkey access and validation is required for HQIP and CHPSO office space. Reports are provided by CHA on a quarterly basis. Cyber Communication did a physical on-site review and validated the security protocols and safeguards as sufficient during the 2022 HIPAA security assessment.	**No Gap** 2021 = Partial Gap

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
		authorized access to the facility where the information system resides and issues authorization credentials for facility access.		
35	Physical Maintenance Records (Standard 10, IS-4)	Documentation of repairs, maintenance and modifications done to maintain or improve the physical security of a facility, such as hardware, walls, doors and locks, is retained according to established policy or vendor requirements.	Building maintenance and hardware updates are not monitored by CAHHS. Locks and the HQIP and CHPSO physical environments are sufficiently secure given the data risk even though a policy to support this requirement does not exist. If building security controls were modified or updated, HIPAA would require the records of such modification be kept for six years.	**No Gap** – No building security upgrades have been done. 2021 = No Gap
36	Physical Workstation Use (Standard 11	Policy and procedures are implemented that specify proper functions to be performed and the way they are to be performed as well as the physical attributes of the surroundings of a specific workstation or class of workstation that can access sensitive information. Access agreements shall include acceptable use provisions and may include nondisclosure agreements and conflict-of-interest agreements. If required by law, regulation or policy, each entity must ensure individuals obtain applicable security clearances. The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	There is a standard for the security of desktops and the ability to view the data on monitors, but it is not formalized by policy. CHA IT does the ordering and configuring of workstations and laptops. HQI HIPAA policies mention screen protectors. Staff ensure monitors are turned away from the entrance to an office even in a work from home environment. This last review period included the procurement and use of HQI (CHA) procured laptops for a work from home environment. These devices all require whole disk encryption and are administratively locked down.	**No Gap** 2021 = No Gap

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
37	Physical Workstation Security (Standard 12)	Physical safeguards are in place at all workstations that access sensitive information to restrict access to authorized users. Each entity shall control access to information system output devices, such as printers and facsimile devices, to prevent unauthorized individuals from obtaining the output of sensitive information.	Workstations and laptops are protected by whole disk encryption. The HQI network is isolated and printers are only mapped to that network. HQI staff cannot see other printers logically. Recently staff were working from home according to COVID-19 requirements. Staff are aware of the requirements to use HQI laptops only for official use.	**No Gap** 2021 = No Gap
38	Physical Device and Media Controls (Standard 13)	Policies and procedures are implemented to govern the receipt and removal of hardware and electronic media that contain sensitive information into and out of a facility, as well as the movement of these items within the facility. Each entity shall safeguard media in digital and/or non-digital form from unauthorized access, use, modification or disposal, inside or outside of the entity's control areas whether in storage or transport. The organization protects and controls the inventory and use of portable devices, ensuring the utilization and authorization is restricted, tracked, and that the devices are sanitized according to policy. NIST 800-111 Encryption of End User Devices NIST 800-88 & DoD 2520.22-M Media Sanitation	HQIP and CHPSO utilize whole disk encryption for systems (the encryption is FIPS 140-2 compliant) and media sanitation to DoD 2520 standards. There are restrictions on removable media by formal policy. Safe Tables have PHI contained in them, but with the exception on one a year, this process has been eliminated and replaced with PHI free webinars. No paper PHI release tracking/authorization exists as a process, but this is not done by procedures outside the HQI environment.	**No Gap** 2021 = Partial Gap Note: One exception to the DoD 2520 sanitation is "potentially" with the cloud provider Otava as the contract does not describe in detail how the data destruction requirements at the end of the contract will be done. This is called out in the BAA ID #29 standard. This requirement should be clearly defined in the next BAA agreement with Otava or alternate cloud provider.

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
39	Physical Information Disposal (Standard 13, IS-1)	Policies and procedures are implemented for the final disposition of sensitive information, and/or the hardware or storage media on which it is stored. Each entity shall sanitize digital and non-digital media prior to disposal in accordance with applicable standards and policies, including media found in devices such as hard drives, mobile devices, scanners, copiers, and printers. The organization sanitizes information system media prior to disposal, using sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies. NIST 800-111 Encryption of End User Devices NIST 800-88 & DoD 2520.22-M Media Sanitation	Hard drives are physically destroyed or use tools to wipe securely (conforming to DoD 5220.22-M standard for erasing or wiping data from a hard drives). HQIP and CHPSO have shredders available for paper destruction. The BAA with Otava states that HQI's data, upon termination of the contract, will be destroyed in the normal course of Otava's data management activities – this is vague language.	**Partial Gap** – Otava (the cloud provider) should be responsible for providing a Certificate of Destruction upon termination of the contract within a specified time period after contract termination. High Impact. Low Cost. 2021 = Partial Gap
40	Physical Media Re-Use (Standard 13, IS-2)	A procedure is implemented for the removal of ePHI from electronic media before it is made available for re-use. Each entity shall sanitize digital and non-digital media prior to release for reuse, in accordance with applicable standards and policies, including media found in devices such as hard drives, mobile devices, scanners, copiers, and printers. The organization sanitizes information system media prior to release out of the organizational control, or release for	CHA IT uses a hardware device or tools to wipe media securely (conforming to DoD 5220.22-M standard for erasing or wiping data from a hard drive). The asset management policy addresses media destruction and reuse. HQIP and CHPSO have not needed to reissue any equipment.	**No Gap** 2021 = No Gap

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
		reuse using sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies and is compliant to NIST 800-88 & DoD 2520.22-M Media Sanitation requirements.		
41	Physical Information Accountability (Standard 13, IS-3)	Documented records of the movements of hardware and electronic media, and the designation of any person responsible for maintaining these records, shall be maintained. The organization maintains accountability for information system media during transport outside of controlled areas and documents activities associated with the transport of information system media. The owner of sensitive information will verify and sign a release authorizing the transfer of information to a third-party validating that security policies and safeguards will be observed prior to the transfer of information and is compliant to NIST 800-88 & DoD 2520.22-M Media Sanitation requirements.	Per the HQI data policy, hardware, software and data that is moved must be approved by the data manager. When sensitive information is released, there is no paper trail or tracking process done; however, this release of ePHI information rarely exists at HQI and has not been done for some time. Laptop movement is not tracked, but they do not contain any PHI data and are whole disk encrypted.	**No Gap** 2021 = Partial Gap
42	Physical Data Backup and Storage (Standard 13, IS-4)	Before equipment is moved, an exact, retrievable copy of the ePHI in it shall be made. Information system backups shall reflect the requirements in contingency plans as well as other entity requirements for backing up information. The organization conducts backups of user-level information contained in the information system.	The very nature of primary storage being located in the Otava cloud vendor's resilient infrastructure satisfies these business requirements. Gaps identified in ID #23 (policies and procedures for data backup) call out the missing data retention policy requirement and this missing policy limits the responsibility for HQI to actively backup and store (retain) backup data for longer than 15 days. CHA IT has Data Protection Manager (only on local machines) and CHA IT backs up everything on the MS	**No Gap** 2021 = Partial Gap

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
			Cloud environment, but that does not include anything in the Otava cloud. There is an Office 365 cloud backup done by CHA IT and stored in the event of a disaster.	
43	Technical Access Control (Standard 14) (#31 is Facility Access Controls)	Technical policies and procedures are implemented to control access to electronic information systems that maintain sensitive information. Access is granted only to authorized persons, as described by the HIPAA Security and Privacy Rules. Each entity shall safeguard access to information assets by managing the identities of users and devices and controlling access to resources and databases on a need-to-know based on the individual's role and position within the organization. Third-parties will also have technical access controls placed on their role and need to have access to the sensitive information or data processing equipment. Access to sensitive information will conform to separation of duties best practices to limit the potential for abuse of privileges.	All CHA IT staff have full administrative access to the HQI local environment. HQI staff cannot make any administrative changes to the HQI desktop or laptop systems assigned to them and maintained by CHA IT. HQIP and CHPSO's environments are physically and logically separated from CHA and other HQI environments via a dedicated firewall system, separate environments, and separate internet access links. The HQIP and CHPSO environments are controlled by role-based user authentication restrictions. Otava has performed SOC 2 audits and attestation of security compliance. They are also culpable to HQI's HIPAA BAA which has access control restrictions defined (Note: Otava has self-re-attested for their compliance to HQI's BAA agreement).	**No Gap** Note: HQI should formalize existing log review requirements that are currently ad hoc, but this finding is located in ID #48. 2021 = Partial Gap
44	Technical Unique User Identification (Standard 14, IS-1)	A unique user identification is assigned for each workforce member requiring access to electronic information systems. The information system uniquely identifies and authenticates organizational and third-party users (or processes acting on behalf of organizational or third-party users) and follows NIST 800-111 (storage only),	Each user has a unique user identification (ID); HQIP and CHPSO do not use any shared user IDs. Systems have unique system ID's as well. There is one common login for the Office 365 cloud administrator account. This should be reviewed for business need (three staff do have access to this login – only for changes in the Office 365 system though).	**Partial Gap** – Each Office 365 System Administration account should be unique and tied to an individual user. Low Impact. Low Cost 2021 = Partial Gap

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
		800-57 and FIPS 140-2 standards as defined in the HQIP and CHPSO business associate agreements.		
45	Technical Emergency Mode Information Access Procedure (Standard 14, IS-2)	Technical means for obtaining access to sensitive information during an emergency have been implemented. The organization develops a contingency plan for the information system that addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure.	There is no business requirement for data access of the SQL data or SAS data for 30 days or more after a disaster. HQIP and CHPSO could access Otava data through a web interface.	**No Gap** 2018 = No Gap
46	Technical Automatic Logoff (Standard 14, IS-3)	A process is implemented to terminate an electronic session after a predetermined period of inactivity. The information system automatically terminates a user session or locks the workstation after some events requiring session disconnect have activated.	Computers have password-protected screensavers that lock after 15 minutes of inactivity. GoToMyPC (used for remote HQI access during COVID-19) is set to five minutes of inactivity. There is no application timeout.	**No Gap** 2021 = No Gap
47	Technical Encryption and Decryption of Data at Rest (Standard 14, IS-4) (See #54 for Transmission Encryption)	A mechanism is implemented for the encryption and decryption of sensitive data at rest. End-to-end storage encryption or approved compensating security control(s) shall be used to protect sensitive information that is stored on portable electronic storage media (e.g., USB flash drives, tapes, CDs, DVDs, disks, SD cards, portable hard drives), mobile computing devices (e.g., laptops, netbooks, tablets, and smartphones), and other electronic devices. The information system implements cryptography in accordance with	Much of the risk for data storage, transmission and integrity have been transferred to their third-party vendor, Otava. It was unclear from the documentation provided by Otava if FIPS-140-2 standards are used in the storage of provider data. Desktops, including laptops, are whole-disk encrypted with BitLocker which is FIPS 140-2 compliant. SQL encryption keys have not been rotated since the installation and NIST limits the maximum usage of an encryption key to two years as a best practice. Stored PSWP's are encrypted by policy. They do not encrypt the SQL server database because it is encrypted at the storage area network level at Otava.	**No Gap** Note: The SQL key rotation should occur every two years as a best practice (unless HQI suspects that it has been compromised). HQI should ensure this practice is in place and audited for compliance, but due to the BAA agreement with Otava, a "No Gap" rating is acceptable. 2021 = No Gap

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
		applicable federal statutes, Executive Orders, directives, policies, regulations, and standards. 800-57 covers managing SQL encryption keys when creating new database keys, creating a backup of the server and database keys, and knowing when and how to restore, delete, or change the keys. NIST 800-111 (storage only), 800-57 and FIPS 140-2 standards are supported with an encryption standard and recommended key management protocols.		
48	Technical Audit Controls (Standard 15)	Hardware, software, and/or procedural mechanisms are implemented to allow examination, or audit, of activity in information systems that contain or use sensitive information. Each entity shall ensure that information systems are capable of being audited and the events necessary to reconstruct transactions and support after-the-fact investigations are maintained.	Audit controls for malicious activity is retained, but inconsistent log review is done to examine the log data that is generated by the Otava cloud environment. Otava log data is retained for six years See as a reactive after-the-fact investigative tool. HQI local network and system log data is retained for 18 months by CHA, but CHA is not a covered entity. HIPAA requires covered entities and business associates to keep logs for up to six years. HQIP and CHPSO HIPAA related audit activity documents are retained and available. Technical (logical) and physical access controls to the SQL data seem to be logged but not proactively reviewed (see ID #18) Internet use is monitored by the MxToolbox service for DNS MX lookups and email blacklists. Office 365 does provide some audit controls and alerts are sent to CHA, but there are no routine periodic reviews. Additional scan services offered by Otava should be investigated.	Partial Gap – No *consistent* periodic audit of the system activity specific to the HQIP SAS and CHPSO SQL applications are done. Note: some elements of this risk are shared with ID #18. High Impact. High Cost. 2021 = Gap

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
49	Technical Storage Integrity (Standard 16)	Technical safeguards are implemented to protect sensitive information (data) from improper alteration or destruction. Information asset owners shall maintain all data records with accuracy, relevance, timeliness, and completeness. Whenever an organization collects personal information, the entity shall maintain the source or sources of the information Automated technical mechanisms (for example digital cyclic redundancy check or checksums) are implemented to protect the integrity of the data stored on any electronic media.	Much of the risk for data storage, transmission and integrity have been transferred to the third-party vendor, Otava. It is unclear how vendors verify data integrity, but they are required to do so based on the BAA. Providers can repopulate the database if needed in the event of a disaster or corruption. There is a policy for integrity and access controls.	**No Gap** 2021 = No Gap
50	Technical Mechanisms to Authenticate Electronic Protected Health Information (Standard 16, IS-1)	Electronic mechanisms (for example digital signatures or checksums) are implemented to corroborate that the integrity of ePHI has not been compromised. The organization employs integrity verification tools to detect unauthorized changes to software, firmware, and information.	Some of the authentication, integrity and access control and integrity have been transferred to the third-party vendor, Otava, based on their BAA. Many data stores use two-factor authentication.	**No Gap** 2021 = No Gap
51	Technical Person or Entity Authentication Mechanisms (Standard 17)	Appropriate mechanisms are implemented to authenticate the identity claimed by the person or entity seeking access to sensitive information. Each entity shall establish processes and procedures to ensure enforcement of password policies or more advanced multifactor mechanisms to authenticate users and devices based on the perceived risk to the information.	Passwords are managed by the system and force a 14-character minimum password length at HQI. Some of the authentication and access control responsibilities have been transferred to the third-party vendor Otava. GoToMyPC and all firewalls have adequate access authentication controls with two-factor authentication.	**No Gap** 2021 = No Gap

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
		The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).		
52	Technical Transmission Security Controls (Standard 18)	Technical security measures are implemented to guard against unauthorized access to sensitive information while it is being transmitted over a network. Each entity shall develop, implement, and document, disseminate, and maintain operational security practices which include, but are not limited to, a network security architecture that includes distinct zones to separate internal, external, and demilitarized zone traffic; and segments internal networks to limit damage, should a security incident occur.	Any data accessible from outside HQIP and CHPSO offices is encrypted, with decryption credentials only given to those authorized for access or via the Otava environment. Much of the risk for data storage, transmission and integrity have been transferred to the third-party vendor Otava via a BAA. Otava uses FIPS-140-2 standards in the transmission of provider data as stated in the older SOC 2 report "Client online sessions are encrypted via HTTPS". (Note: the physical protection of digital certificate has not been verified by the independent SOC reports, a critical part of FIPS-140-2). SFTP encryption from Otava is covered in ID #54. CHA manages HQI's environments on HQI's local area network (LAN), wide area network (WAN), and demilitarized zone (DMZ) environments and they are separated from CHA's environment. There are no systems located in the DMZ. A dedicated firewall monitors all data access and data leaving the HQI and CHPSO network, Alerts are sent, but no proactive monitoring of the logs is being done. Data protection and data loss prevention capabilities are natively built into Office 365 and the Cisco Meraki tool. Portable document format (pdf) files have the option to be encrypted using a FIPS 140-2 compliant encryption.	**No Gap** 2021 = No Gap

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
53	Technical Transmission Integrity Controls (Standard 18, IS-1)	Controls are in place to ensure the integrity of sensitive data in transmission and that it is not improperly modified without detection until it can be disposed of. Information asset owners shall apply all applicable information security law, policies, standards, and procedures to protect personal information under the information asset owner's responsibility. The information system protects the integrity of transmitted information.	Much of the risk for data storage, transmission and integrity have been transferred to HQI's third-party vendor Otava via a BAA. GoToMyPC is encrypted and protects transmission integrity. Otava uses FIPS-140-2 standards in the transmission of provider data as stated in the older SOC 2 report "Client online sessions are encrypted via HTTPS". (Note: the use of encryption protects data integrity in transmission as part of the FIPS-140-2 standard).	**No Gap** 2021 = No Gap
54	Technical Transmission Encryption (Standard 18, IS-2) (See #47 Encryption and Decryption of Data at Rest)	Where appropriate, sensitive data is encrypted to protect its confidentiality and integrity as it is transmitted. End-to-end encryption or approved compensating security control(s) shall be used to protect sensitive information that is transmitted or accessed outside the secure internal network (e.g., email, remote access, file transfer, Internet/website communication tools) of the entity The information system protects the confidentiality of transmitted information. 800-57 managing transmission encryption keys consists of creating new symmetric or asymmetric key pairs (PKI), creating a backup of the keys, and knowing when and how to restore, delete, or change the keys. FIPS 140-2 standards are supported with an encryption standard and	Much of the risk for data storage, transmission and integrity have been transferred to HQI's third-party vendor Otava via a BAA. Otava uses FIPS-140-2 standards in the transmission of provider data as stated in the older SOC 2 report "Client online sessions are encrypted via HTTPS". Microsoft email has a method to encrypt email in transit, but it is not currently used. During the COVID-19 pandemic staff used a VPN client to connect to the Otava system for work in the cloud via a multi-factor authentication tool. GoToMyPC remote access and a Fortinet VPN is also used to connect to Otava and the HQI environment. HQIP and CHPSO are on their own firewalled network and other CHA staff cannot get to the HQI network (the exception is the four CHA IT staff who need access for IT services on the HQI network). MS email filtering has the capability to encrypt email in transit, but it is not turned on automatically.	**No Gap** 2021 = No Gap

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
		recommended key management protocols		
A	PSQIA 42 CFR Part 3 - PATIENT SAFETY WORK PRODUCT	Patient Safety Work Products are protected from disclosure. **Disclosure** means the release, transfer, provision of, access to, or divulging in any other manner of "Non-Safe Harbor" Patient Safety Work Product information. In order to meet the standard for nonidentification in accordance with 42 CFR §3.212, all of the 18 identifiers and any event codes, reports or feedback contained in the patient safety evaluation system must also be considered ePHI and protected.	Patient Safety Work Products still contain PHI, but are secured and encrypted while in storage (at rest) in a way that prevents it from disclosure. Per the HQI data policy, all data users with access to confidential ("non-Safe-Harbor") data must sign a confidentiality agreement with the data owner. Safe Tables/Patient Safety Work Products (PSWP) do contain PHI, but there is only one done each year and all participants have signed NDAs prior to attending. Webinars have replaced PSWPs and do not contain any patient data or any of the 18 HIPAA identifiers. Microsoft Defender does have a feature to identify and scan for protected information on the HQI SharePoint Office 365 Message Encryption allows users to send encrypted email from Outlook and Outlook on the web. Zip Codes, dates of birth, event reports and feedback are still considered to be ePHI (please see: https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#zip) and, if included in data, emails or feedback, it does meet the requirements of "Safe Harbor" and must be encrypted at rest and in transit.	**No Gap** 2021 = Partial Gap
B	PSQIA, § 3.106(b)(2) Sensitive provider information is firewalled from standard business information.	PSO's data and functions are logically or physically separated and access is controlled. Users without need-to-know patient data are segregated to the business environment and have no access to the Protected Individually Identifiable (ePHI) information.	CHPSO and HQIP have distinctly different applications and virtual machines in the Otava environment. HQI is firewalled from the CHA environment, but CHA IT has technical support responsibilities over HQI. This does not seem to cause any conflict, but log reviews are not done periodically to confirm this (see ID #48).	**No Gap** **2021 = No Gap**

ID #	Standards & Implementation Specifications (IS)	Description of a Compliant State	HQIP / CHPSO's Current Status	Gap, Safeguard Action, Impact & Qualitive Cost Estimate[8]
C	CMIA, any data that is deidentified or aggregated must be done in a way that is consistent with the HIPAA Privacy Rule.	Per the HHS guidelines to fully utilize the "Safe Harbor" safeguard, covered entities may include the first three digits of the zip code if, according to the current publicly available data from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people CMIA utilizes the "Safe Harbor" definition from the HIPAA Privacy Rule to describe data that has been sufficiently deidentified to allow it to be stored, transmitted and used in an unencrypted way. Any data that does not meet this definition must be appropriately encrypted.	CHPSO data does meet the requirement for Safe Harbor consistent with the HIPAA Privacy Rule, and is safeguarded to a level that would be compliant to the CMIA law. BAAs do not contain CMIA language, but Otava does encrypt data at rest and in transit per SOC2 independent assessments. HQIP does not use any ePHI data in its work process.	**No Gap** Some CMIA gap elements are identified and accounted for in ID #29. **2021 = No Gap**

Attachment 2 - Interview List

Cyber Communication interviewed or received input from the following individuals during the course of this project:

- Alex Baskett
- Robert Imhoff
- Scott Masten
- Tim Rehwald
- Julie Reppas
- Vivian Eusebio
- Kimberly Beard
- Brianna Parker
- Allison Bradley

Attachment 3 - Documents Reviewed List

The following documents were reviewed during the course of this project:

- FR Secure Vulnerability Scan
- Confidentiality Training PowerPoint
- CHPSO Policies and Procedures V1.docx
- HQI Patching Matrix V3.xlsx
- HQI Protected Data Security Policies 04012022.docx
- HQI Protected Data Security Policies 11012021.docx
- CAHHS Policy Manual October 2021
- Business Associate “Boilerplate” template and various BAAs
- Various device logs and tracking spreadsheets
- Log Inspection Rules (Routing, Windows, Terminal Services) documents
- Protected Health Information Data Governance Structure 04022020.pdf
- Security and Confidentiality Acknowledgement 04022020.docx
- Otava HQI_SOC 1 Type 2 Report 7/21/2021
- Otava HQI_SOC 2 Type 2 Report 7/21/2021
- Otava HQI_SOC 2 Type 2 Report 7/21/2021
- HQI - Otava - SOC 2 - Bridge or GAP Letter (self-attestation letter) 3/1/2022
- Otava HQI_HIPAA HITECH Attestation Report Expired 7/21/2019
- Cyber Communication CHPSO HIPAA Security Assessment Report 01/13/2021
- HQI internal Log Review history
- HQI Protected Health Information Data Governance Structure
- Dual Authentication setup
- Otava User ID Decommission Process
- HQI Protected Data Security and Confidentiality Agreement

Attachment 4 – Legacy 2020 Compliance Tables

2020 Table 1: Overview and Compliance States Defined

Compliance State	2020 Percent Compliance	Sufficiency Principles	Visual Indicator for Table 2
No Gap	55.5%	Safeguard requirements are fully met.	
Partial Gap	32%	Safeguard is insufficient but meaningful progress towards compliance has been made.	
Gap	12.5%	Safeguard is insufficient	

2020 Table 2: Security Compliance Dashboard

Standards (Std) & Implementation Specifications (IS)		Compliance Status					
		Std (A)	IS-1 (B)	IS-2 (C)	IS-3 (D)	IS-4 (E)	IS-5 (F)
HIPAA Administrative	22. Security Management Process	PG	G	PG	N	G	
	23. Assigned Security Responsibility	N					
	24. Workforce Security	N	N	N	N		
	25. Information Access Management	N	N/A	N	N		
	26. Security Awareness and Training	N	N	G	PG	PG	
	27. Security Incident Procedures	PG	PG				
	28. Contingency Plan	G	PG	G	N	G	N
	29. Evaluation of Security Procedure	PG					
	30. Bus. Assoc. Contracts or Other Arrangements	PG	PG				
Physical	31. Facility Access Controls	N	N	N	PG	N	
	32. Workstation Use	N					
	33. Workstation Security	N					
	34. Device and Media Controls	PG	PG	N	PG	PG	
HIPAA Technical	35. Access Control	PG	PG	N	N	N	
	36. Audit Controls	G					
	37. Integrity Controls	N	N				
	38. Person or Entity Authentication	N					
	39. Transmission Security	N	N	N			
CMIA & PSQIA	40. PSQIA – Disclosure of non-Safe Harbor data	PG					
	41. PSQIA – Data Logically Separated	N					
	42. CMIA – Sensitive Data is Appropriately Encrypted	N					

Attachment 5 – Legacy 2018 Compliance Tables

2018 Table 1: Overview and Compliance States Defined

Compliance State	Percent Compliance	Sufficiency Principles	Visual Indicator for Table 2
No Gap	46%	Safeguard requirements are fully met.	
Partial Gap	31%	Safeguard is insufficient but meaningful progress towards compliance has been made.	
Gap	23%	Safeguard is insufficient	

2018 Table 2: Security Compliance Dashboard

	Standards (Std) & Implementation Specifications (IS)	Compliance Status					
		Std (A)	IS-1 (B)	IS-2 (C)	IS-3 (D)	IS-4 (E)	IS-5 (F)
Administrative	1. Security Management Process	G	G	G	N	G	
	2. Assigned Security Responsibility	PG					
	3. Workforce Security	N	PG	N	N		
	4. Information Access Management	N	N/A	N	N		
	5. Security Awareness and Training	N	N	PG	PG	G	
	6. Security Incident Procedures	G	PG				
	7. Contingency Plan	G	N	G	N	G	N
	8. Evaluation of Security Procedure	PG					
	9. Bus. Assoc. Contracts or Other Arrangements	PG	G				
Physical	10. Facility Access Controls	N	N	N	PG	N	
	11. Workstation Use	PG					
	12. Workstation Security	N					
	13. Device and Media Controls	PG	PG	PG	PG	PG	
Technical	14. Access Control	PG	N	N	N	PG	
	15. Audit Controls	G					
	16. Integrity Controls	N	N				
	17. Person or Entity Authentication	N					
	18. Transmission Security	N	N	G			

	G	= Gap	PG	= Partial Gap	N	= No Gap	N/A	= Not Applicable