AGENDA

BAY ARENAC BEHAVIORAL HEALTH
BOARD OF DIRECTORS
CORPORATE COMPLIANCE COMMITTEE MEETING

Thursday, August 6, 2026 at 5:00 pm

Room 225, Behavioral Health Center, 201 Mulholland Street, Bay City, MI 48708

	Committee Members:	Present	Excused	Absent	Committee Members:	Present	Excused	Absent	Others Present:
	Patrick Conley, Ch				Shelley King				BABH: Melissa Prusi, Christopher Pinter, and Sara McRae
	Pam Schumacher, V Ch				Patrick McFarland, Ex Off				
	Tim Banaszak				Robert Pawlak, Ex Off				Legend: M-Motion; S-Support; MA-Motion Adopted; AB-Abstained
	Christopher Girard								

	Agenda Item	Discussion	Motion/Action
1.	Call to Order & Roll Call		
2.	Public Input (Maximum of 3 Minutes)		
3.	Unfinished Business 3.1) None		
4.	New Business 4.1) Corporate Compliance Report 4.2) Corporate Compliance Committee Notes from the meetings dated: a) April 13, 2026 b) May 11, 2026 4.3) Corporate Compliance Semi-Annual Report 4.4) Quarterly Fraud & Abuse Report to Midstate Health Network (MSHN)		4.1) No action necessary 4.2) No action necessary 4.3) No action necessary 4.4) No action necessary

AGENDA

BAY ARENAC BEHAVIORAL HEALTH
BOARD OF DIRECTORS
CORPORATE COMPLIANCE COMMITTEE MEETING
Thursday, August 6, 2026 at 5:00 pm
Room 225, Behavioral Health Center, 201 Mulholland Street, Bay City, MI 48708

	4.5) 2025-2026 Information Management Strategic & Operational Plan Revisions		4.5) Consideration of a motion to refer the revisions to the 2025-2026 Information Management Strategic & Operational Plan to the full board for approval
	4.6) Strategic Initiatives & Revised Dashboard Review		4.6) No action necessary
5.	Adjournment	M - S - pm MA	

BAY-ARENAC BEHAVIORAL HEALTH
BABHA CORPORATE COMPLIANCE COMMITTEE MEETING
Monday, April 13, 2026 (1:00 - 3:00 pm)

MEMBERS	Present	MEMBERS	Present	MEMBERS	Present
Amy Folsom, Clinical Program Manager	-	Joelle Sporman, BI Secretary (Recorder)	-	Sarah Holsinger, Quality Manager	-
Heather Friebe, Integrated Care Director, Arenac	X	Karen Amon, Directory of IHC	X	Stephanie Gunsell, Contract Manager	X
Jackie Kish, RR/CS Manager	-	Marci Rozek, Chief Financial Officer	X	**GUESTS**	**Present**
Jennifer Lasceski, Director of HR	X	Melissa Prusi, Compliance & Privacy Officer (Chair)	X	Lynn Meads, Records Specialist (recorder)	X
Melissa Prusi, Security Officer	X	Michele Perry, Finance Manager	X		
Joelin Hahn, Director IHC	-	Nicole Sweet, Director of IHC	X		

#	Topic	Key Discussion Points	Action Steps
1.	a) **Agenda**: Review/Additions b) **Meeting Notes**: Approval of March 9, 2026, meeting notes c) **Next Meeting**: May 11, 2026	a) The agenda was reviewed with no additions or changes. b) March 9, 2026, meeting notes were reviewed and approved as written. c) The next meeting is scheduled for May 11, 2026.	
2.	**State-Federal Laws, MDHHS Notices and Regulations:** a) Review of Log and Subject Matter Expert Report Outs	a) Review of Log and Subject Matter Expert Report Outs – Melissa and the committee reviewed the log (Log can be found at G:\BABH\Corp Comp Regs-Codes-Manuals - CC Committee Law-Reg Mgt Log). Log Issue 447 – WHODAS Announcement - No updates to report. Log Issue 451 – MSHN CFA & P Next Steps Plan – Central CMH is piloting. Added to HSW waiver. Policy re: CFA & Planning developed, approved and enacted. MSHN also has a CFA&P policy. Waiting to see if it's going to be enacted which could impact what our current processes are. Log Issue 452 – SEDW and MichiCANS/CAFAS update – No updates. Log Issue 453 – Autism Diagnosis HB4146 - No updates to report.	

#	Topic	Key Discussion Points	Action Steps
		Log Issue 464 – Medicaid/HSW SD arrangements for CLS - To be closed. Log Issue 465 – Medicaid/HSW-SD budget process - No updates to report this month. Continue to monitor. To be Closed Log Issue 474 – SB 413 Psychologist supervision - No updates. Log Issue 475 – SB 219 AOT Bills - Some movement. Jill indicated the House approved and it went back to the Senate. No formal approval. Log Issue 477 – Senate Bill 220 - No updates to report this month. The package went back to the senate. Continue to monitor. Log Issue 478 – Senate Bill 221 - No updates to report this month. Continue to monitor. Log Issue 479 – Mental Health Framework – No updates to report this month. Continue to monitor. Log Issue 481 – HB 4727-4729 Proposed guardian and conservator licensure requirements - No updates to report this month. Continue to monitor. Log Issue 488 – HCBS Final Rule, Person-Centered Planning –Still working on this. The issue of compliance with the attestations from CSM/Supervisors. Have to look at changes to EHR to address the 8 elements Log Issue 495 – 2549-EVV-p EVV Compliance Standards - Must determine access to reports sent out monthly to admins. For April CMHSPs must send compliance reports to the PIHP. EVV meeting on Wednesday to discuss reporting/compliance issues. IT dept may be discussing this. Karen to reach out to Todd for follow-up to determine who is to be receiving the reports at MSHN. Michele to reach out to Leslie T at MSHN to see if she is aware.	Log Issue 495: Karen to reach out to Todd L. for follow-up to determine who is to receive reports at MSHN. Michele to reach out to Leslie T at MSHN.

#	Topic	Key Discussion Points	Action Steps
		Log Issue 498 – HB4032 removes interstate medical licensure compact sunset - Close. Log Issue 502 – CMHA Legislature HB 5074 – It modified renewal limits for temporary limited mental health licenses. Continue to Monitor. Melissa to send to Jennifer for review. Log Issues 502-532 – FYI - Melissa went through the logs as a FYI. See Log for more information. Log Issue 533 – CPS Release of information. The main difference is it went from 14 days to 7 days. Melissa to follow up to make sure everything is compliant with BABH policy. Log Issue 534 – HSW Waiver Amendment – MDHHS Final Bulletin. Melanie reported at PNOQMC there is no revised training so they will have to take the initial one again. The training for our CSMs and provider network is in June. Log Issue 535 – Training Requirements for MMHC children's Diagnostic and Treatment. Leadership was given this information. Relias dates will be changed to fiscal and pro-rated. To be removed. Log Issue 536 – 1915(b) MiChoice Waiver Amendment. This waiver amendment has several changes, one being to allow surveillance cameras in common areas of AFC homes for Aged, and unlicensed assisted living settings. This does not apply to BABH. Some of the changes are in contradiction to what our waivers require. To be Removed. Log Issue 537 – CCBHC Demonstration Direct Payment Transition -2552 BH-P. Talks about the CCBHC Demonstration requirements related to direct pay. Policy updates, provider enrollment, bill and reimbursement requirements related to the payment model transition. To be Closed.	Log Issue 502: Mel to send to Jennifer for review. Log Issue 533: Melissa to review Policy to ensure we are compliant with 7-day notification.

#	Topic	Key Discussion Points	Action Steps
		Log Issue 538 – Home Help Compliance Review - 2602-HH-P. Home Help new agency provider compliance review and home help random audits. This may trickle forward to CLS through EVV. To be Closed. Log Issue 539 – Standardized mental health assessment requirements -Final Bulletin MMP 26-01-BH-Final. Standardized tools: MichiCANS screener for birth to 18, LOCUS for 18+. These must be completed by QMHP, CMHP, or QIDP. Monitoring. Log Issue 540 – Master's level temporary Limited Licensed Psychologists, LL Counselors, Educational LL Marriage and Family Therapists, and LLMSWs. - 2554-BH-P. Effective August 1, 2026. The implementation of portions of the policy is contingent upon approval of an SPA by CMS. LL Behavioral health providers must complete an online application for CHAMPS. LL Behavioral health providers must enroll as "Rendering Only". To be Closed Log Issue 541 – Behavioral Health Treatment requirements for Autism Services - 2613-BCCHPS-P. Proposed effective date June 1, 2026. Update BHT Autism Services: aligning policy language with generally accepted standards of care for best practice in ABA. Removes the requirement for a PE by a PCP prior to receiving BHT services. Adding language to increase access to qualified licensed diagnosticians as approved by MDHHS and updating BHT service provider qualification language to align with requirements per LARA. Monitoring. Joelin to review. Log Issue 542 – MI Coordinated Health (MICH) - 2511-MICH-P – Introduction of a new MI Coordinated Health chapter within the MPM effective January 1, 2026. Karen reviewed. Does not pertain to BABH. Closed. Log Issue 543 – HB 4536: This talks about an insurer that delivers, issues for delivery, or renews in this state a health insurance policy shall not deny, modify, or delay a claim based on a review using AI.	Log Issue 539: Nicole and Joelin to review. Log Issue 541: Joelin to review.

#	Topic	Key Discussion Points	Action Steps
	b) Review of CMHA Update on Legislative and Policy Changes c) Review of Compliance Updates/Regulatory Education Needed for Staff d) Process for Ensuring Implementation of Policy Changes e) Updates from CMHAM ED Forum	b) <u>Review of CMHA Update on Legislative and Policy Changes</u> – See above. c) <u>Review of Compliance Updates/Regulatory Education Needed for Staff</u> – See above. d) <u>Process for Ensuring Implementation of Policy Changes</u> – See above. e) <u>Updates from CMHAM ED Forum</u> – • Wage Coalition Explainer – Protect MI Direct Care Worker Wages – reviewed handout. • Financial Exploitation Bill Package – reviewed handout. • Application for 1915(C) HCBS HSW Waiver Amendment – CMHA Study and Comments on the Proposed Policy – reviewed handout. • Medicaid Spenddown Discussion – reviewed handout. • CMHA Comments re: 2613-BCCHPS – reviewed handout. • ICSS Crisis Hub – CMHA comments – reviewed handout.	
3.	**<u>Plans, Policies, Procedures, Assessments</u>:** a) Status of Employee Attestations/Time for new ones (end of Summer/early Fall)	a) <u>Employee Attestations</u> – No updates.	a) <u>Employee Attestations</u> – Melissa to reach out to staff that were on vacation/leave.
4.	**<u>Data/Monitoring/Reports</u>:** a) Phoenix and Gallery Breach Monitoring b) Exclusion/Debarment – Officers, Employees, Contractors, Vendors (Annual staff Attestation for Fraud /Abuse/ Convictions during Staff Development Days)	a) <u>Phoenix and Gallery Breach Monitoring</u> –There were no security breaches in Phoenix or Gallery for the month of March. b) <u>Exclusion/Debarment</u> – There were no findings to report this month. No exclusions/debarments.	

#	Topic	Key Discussion Points	Action Steps
	c) Monitoring of Group Drives for Unsecured PHI Files d) Security Officer Update e) Ethics/Recipient Rights/Customer Service Update f) Report on spot checks for compliance for Self Determination g) Corporate Compliance Activity Report – Summary of log **<u>April Reports:</u>** h) Email Security Phishing drills	c) <u>Monitoring for Unsecured PHI Files</u> – No unsecured PHI. d) <u>Security Officer Update</u> – Two security incidents – mild and corrected. Two devices discovered that did not have 2-factor authentication. e) <u>Ethics/RR/CS Update</u> – Jackie reported there were no HIPAA/Confidentiality complaints for FY26Q2. Ethics meeting is 04/29/2026 f) <u>Report on spot checks for SD</u> – Ben reported that he reviewed 6 sets of notes and provided education regarding IPOS improvement. One education regarding duplicate notes. Two new referrals. One education/feedback regarding progress notes. g) <u>Corporate Compliance Activity Report</u> – Some MEV reviews resulting in recoupments, mainly human error. No trends regarding HIPAA issues. h) <u>Email Security Phishing drills</u> – March drills resulted in 18% click rate which is higher than acceptable industry standards. Each member of staff received immediate education with the Hook system as well as being assigned Relias training.	
5.	**<u>Outstanding Items/Other</u>** a) None	Nothing to address this month.	
6.	**Adjourn**	**The next meeting is scheduled for Monday, May 11, 2026, from 1:00 - 3:00 pm via MS Teams.**	

BAY-ARENAC BEHAVIORAL HEALTH
BABHA CORPORATE COMPLIANCE COMMITTEE MEETING
Monday, May 11, 2026 (1:00 - 3:00 pm)

MEMBERS	Present	MEMBERS	Present	MEMBERS	Present
Amy Folsom, Clinical Program Manager	X	Joelle Sporman, BI Secretary (Recorder)	-	Sarah Holsinger, Quality Manager	X
Heather Friebe, Integrated Care Director, Arenac	X	Karen Amon, Directory of IHC	X	Stephanie Gunsell, Contract Manager	X
Jackie Kish, RR/CS Manager	X	Marci Rozek, Chief Financial Officer	X	**GUESTS**	**Present**
Jennifer Lasceski, Director of HR	X	Melissa Prusi, Compliance & Privacy Officer (Chair)	X	Lynn Meads, Records Specialist (recorder)	X
Melissa Prusi, Security Officer	X	Michele Perry, Finance Manager	X		
Joelin Hahn, Director IHC	X	Nicole Sweet, Director of IHC	X		

#	Topic	Key Discussion Points	Action Steps
1.	a) **Agenda**: Review/Additions b) **Meeting Notes**: Approval of April 13, 2026, meeting notes c) **Next Meeting**: June 8, 2026	a) The agenda was reviewed with no additions or changes. • Melissa reached out requesting feedback regarding meeting improvement and productivity. Please email Melissa with any suggestions. b) April 13, 2026, meeting notes were reviewed and approved as written. c) The next meeting is scheduled for June 8, 2026.	
2.	**State-Federal Laws, MDHHS Notices and Regulations:** a) Review of Log and Subject Matter Expert Report Outs	a) Review of Log and Subject Matter Expert Report Outs – Melissa and the committee reviewed the log (Log can be found at G:\BABH\Corp Comp Regs-Codes-Manuals - CC Committee Law-Reg Mgt Log). Log Issue 447 – WHODAS Announcement - No updates to report. Log Issue 451 – MSHN CFA & P Next Steps Plan – Central CMH is piloting. Added to HSW waiver. Policy re: CFA & Planning developed, approved and enacted. MSHN also has a CFA&P policy. Updated HSW policies note CFA&P. Monitoring Log Issue 452 – SEDW and MichiCANS/CAFAS update – No updates.	

#	Topic	Key Discussion Points	Action Steps
		Log Issue 453 – Autism Diagnosis HB4146 - No updates to report. Log Issue 474 – SB 413 Psychologist supervision - No updates. Log Issue 475 – SB 219 AOT Bills - Some movement. Jill indicated the House approved and it went back to the Senate. No formal approval. No Updates Log Issue 477 – Senate Bill 220 - No updates to report this month. The package went back to the senate. Continue to monitor. No updates Log Issue 478 – Senate Bill 221 - No updates to report this month. Continue to monitor. No updates. Log Issue 479 – Mental Health Framework – CMHA advocating against this. OP ED vilifying the MHF. Appropriations members added language to the boilerplate language opposing this. Continue to monitor. Log Issue 481 – HB 4727-4729 Proposed guardian and conservator licensure requirements - No updates to report this month. Continue to monitor. Log Issue 488 – HCBS Final Rule, Person-Centered Planning – Closed. Log Issue 495 – 2549-EVV-p EVV Compliance Standards - Must determine access to reports sent out monthly to admins. For April CMHSPs must send compliance reports to the PIHP. Quarterly reports sent out to providers. Michele received an email from Joseph Wagner, Tech Project Manager, stating he had access to all the CMH reports and would not need it to be sent to him. Otherwise, no updates. Log Issue 502 – CMHA Legislature HB 5074 – It modified renewal limits for temporary limited mental health licenses. Continue to Monitor. Melissa to send to Jennifer for review.	Log Issue 502: Mel to send to Jennifer for review.

#	Topic	Key Discussion Points	Action Steps
		Log Issue 533 – CPS Release of information. The main difference is it went from 14 days to 7 days. Joelin to review notes from MSHN CLC emails regarding this. Log Issue 534 – HSW Waiver Amendment – MDHHS Final Bulletin. Annual training due in June. Will have to retake same training as it was not updated. Log Issue 535 – Training requirements for MMHC Children's Diagnostic and Treatment. Staff development making amendments to shift due date to being September 30 because it is now being moved to fiscal year from calendar year. Closed. Log Issue 539 – Standardized mental health assessment requirements -Final Bulletin MMP 26-01-BH-Final. Standardized tools: MichiCANS screener for birth to 18, LOCUS for 18+. These must be completed by QMHP, CMHP, or QIDP. Limited License must be supervised under a fully licensed provider of the same profession and Bachelor's Level Providers may Assist in conducting assessments under the licensure and supervision of an allowable MHP provider. Monitoring. Log Issue 544 - CPT & HCPCS Update – MMP 26-15 – Michele and Joelin have a meeting with MSHN leads regarding changes tomorrow prior to providing guidance to providers. Updates included: • U5 modifier dropped. • Y1 modifier added to H2015 – Prolonged exposure • Z1 modifier added to H2021 Motivational interviewing for adolescents. • 97155 – cost considerations noted "must co-occur w/ 97153, 97154 and H0373T" now reads it "may co-occur with 97153 & 97154". Log Issue 540 – HCBS 1915 (i)SPA – MMP 26-12. P&Ps are set, Karen will review to be sure.	Log Issue 533: Joeline to review notes from MSHN CLC emails. Log Issue 544: Michele and Joelin to report back with findings after MSHN mtg. Log Issue 540: Karen to review P&P

#	Topic	Key Discussion Points	Action Steps
	b) Review of CMHA Update on Legislative and Policy Changes c) Review of Compliance Updates/Regulatory Education Needed for Staff d) Process for Ensuring Implementation of Policy Changes e) Updates from CMHAM ED Forum	Log Issue 541 – Behavioral Health Treatment requirements for Autism Services - 2613-BCCHPS-P. Proposed effective date June 1, 2026. Log Issue 545 – 1915 HSW – Bulletin MMP 26-14 – Home and Community Based (HCBS) 1915(i) State Plan Amendment. Proposed effective date June 1, 2026. Please see Bulletin in CCC Folder for full list of changes. Main concern is the WHODAS being identified as replacement to the SIS, unless there is an active SIS. No direction regarding implementation of WHODAS from MDHHS. b) Review of CMHA Update on Legislative and Policy Changes – See above. c) Review of Compliance Updates/Regulatory Education Needed for Staff – See above. d) Process for Ensuring Implementation of Policy Changes – See above. e) Updates from CMHAM ED Forum: No updates	Log Issue 541: Joelin to review and report at next CCC.
3.	**Plans, Policies, Procedures, Assessments:** a) Status of Employee Attestations/Time for new ones (end of Summer/early Fall)	a) Employee Attestations – 210 / 253 employees completed.	a) Employee Attestations: Mel to send another update to include employees and their supervisors.
4.	**Data/Monitoring/Reports:** a) Phoenix and Gallery Breach Monitoring b) Exclusion/Debarment – Officers, Employees, Contractors, Vendors (Annual staff Attestation for Fraud	a) Phoenix and Gallery Breach Monitoring – No breaches b) Exclusion/Debarment – No findings c) Monitoring for Unsecured PHI Files – No unsecured PHI.	

#	Topic	Key Discussion Points	Action Steps
	/Abuse/ Convictions during Staff Development Days) c) Monitoring of Group Drives for Unsecured PHI Files d) Security Officer Update e) Ethics/Recipient Rights/Customer Service Update f) Report on spot checks for compliance for Self Determination g) Corporate Compliance Activity Report – Summary of log **<u>May Reports:</u>** h) Verification of Medicaid Services direct operated & contracted service providers. i) Provider Network Site Review Summary	d) <u>Security Officer Update</u> – Melissa will be reviewing SRA with all of IT and reviewing some issues that were pointed out in that SRA and remediation with extended SLT. e) <u>Ethics/RR/CS Update</u> – Ethics Committee canceled due to lack of issues to address. No RR complaints regarding compliance/confidentiality issues. Potential issue regarding Centria recording all calls. f) <u>Report on spot checks for SD</u> – • April – No new referrals • Trained 2 staff on an old Plan that Quality reviews indicated there was a gap. IPOS Training Forms cause a lot of headaches when the process is slowed. • One case of Over-utilization but they are adults with other supports so no additional hours added. • SDC reviewed 13 sets of Notes for April. Many of them were for IPOS preparation and SDC was able to provide on-the-spot feedback even if the notes were acceptable. There was one set of notes that SDC questioned if there was potential copy/pasted. Consulting with Quality regarding this. Most notes were good quality or at least adequate. g) <u>Corporate Compliance Activity Report</u> –No complaints regarding privacy, security, or any confidentiality that needed looked into and no actual fraud and abuse or potential fraud and abuse reported. Overall, trends were basically MEV reviews with some documentation issues h) <u>Verification of Medicaid Services direct operated & contracted service providers</u>. Nothing to report. i) <u>Provider Network Site Review Summary:</u> For Q2 we are currently doing specialized residential. In Q1 completed new dietary services, the Opportunity Center and the remaining ABA.	

#	Topic	Key Discussion Points	Action Steps
	j) Plan w/in 15 days; Health Care Coord; Crisis Planning; Medical Necessity k) Ability to Pay Compliance Rate	j) <u>Plan w/in 15 days; Health Care Coord; Crisis Planning; Medical Necessity</u>. For Plan within 15 days, Data analysis shows MPA at 82% (9% decrease from FY25Q4), Bay Direct at 87% (2% decrease from FY25Q4), SPSI at 71% (16% decrease from FY25Q4) and List at 100% (50% increase from FY25Q4. For Health Care Coord, Data analysis shows Bay Direct % 85% (1% decrease from FY25Q4, SPSI at 93% (9% increase from FY25Q4), List at 85% (2% decrease from FY25Q4) and MPA at 82% (2% increase from FY25Q4). k) <u>Ability to Pay Compliance Rate</u> – PCE changed reports and will not be doing this anymore. So, may not need to review this in upcoming meetings.	
5.	**<u>Outstanding Items/Other</u>** a) None	Nothing to address this month.	
6.	**Adjourn**	**The next meeting is scheduled for Monday, June 8, 2026, from 1:00 - 3:00 pm via MS Teams.**	

BAY ARENAC BEHAVIORAL HEALTH

Corporate Compliance Report

FY26 Quarter 2 through FY26 Quarter 3

Scale for Status Rating: Good-Improved-Fair-Poor

COMPLIANCE MONITORING

Monitoring	Status at Last Report	Status as of this Report	Comments
Electronic health record security breach monitoring (for violations of role-based security)	Good	Good	No findings.
Sanctioned provider (exclusion/ debarment) checks for employees and officers, contracted clinical service providers and selected vendors	Good	Good	No findings.

Auditing	Status at Last Report	Status at this Report	Comments
Contracted Service Provider Site Reviews	Good	Good	During FY25Q1 and FY25Q2 site reviews were completed for Community Living Supports, Self-Direction, Private Duty Nursing, Specialized Residential (out of county), Occupational Therapy, Speech Language Pathology, Physical Therapy, Psychosocial Rehabilitation, and Dietary service providers.
Record Reviews	Good	Good	FY26Q1- 94.8% of records assigned were completed. 89% trainings were completed. Areas falling under the threshold included Coordination of care not evident, IPOS not reviewed for effectiveness within the time frames indicated. This was an improvement from FY25 Q4. FY26Q2- 85% of records assigned were completed. 93% trainings were completed. Areas falling under the threshold included the Termination/transfer sections were not completed accurately, IPOS not reviewed for effectiveness within the time frames indicated, all sections of the IPOS were not completed, all sections of the assessment were not completed and coordination of care not evident. Overall this is on trend from FY25Q4.
Verification of Medicaid services provided for direct operated programs & contracted service providers	Good	Good	In FY26Q1 and FY26Q2, there were 6,800 claims reviewed for tertiary services. Of those 6,800 claims reviewed, there were 152 claims found with errors. This resulted in a 97.8% compliance rate. These reviews included Community Living Supports, Self-Direction, Private Duty Nursing, Specialized Residential (out of county), Occupational Therapy, Speech Language Pathology, Physical Therapy, Psychosocial Rehabilitation, and Dietary service providers. Trends noted for these reviews included missing documentation, wrong start/stop time, and incorrect number of units submitted. For primary service providers, including BABH, there were 411 claims reviewed with 5 errors, resulting in a 99.2% compliance rate. Self Determination Coordinator has been completing monthly spot checks for MEV and quality in documentation and reporting to the CCC.

RISK ASSESSMENT			Status of Action Plans
Dep't of Justice Compliance Program Eval	Triennial	Next eval due in 2025 – pushed back to 2026	The 2022 self-evaluation was completed during the reporting period as scheduled. BABHA scored 99-100% on 34 out of 43 standards (80%). Of the 9 standards warranting improvement, action steps include more training for supervisors on compliance, strengthening training on policies and procedures, and post implementation evaluation of process changes to ensure regulatory

RISK ASSESSMENT			Status of Action Plans
			compliance is fully actualized. Training for Supervisors has been developed and individual new supervisors have had one on one training. To address education on policies and procedures this has been incorporated in the Relias System. The DOJ Evaluation is in process now and will be completed by 09/30/2026.
Fraud/Abuse Risk Assessment	Triennial	Next Assessment due 12/2026	Completed and presented to CCC 12/2023. Presented and Approved by HCICC 1/2024. The MEV reviews have been completed as scheduled and the increased amount of MEV's being conducted has been implemented. The external providers have been restricted from being able to do stand alone authorizations. A report for expired IPOS is available to external providers now that everyone is on PCE. The Self Determination Coordinator has provided monthly MEV and provider education and reported this to the CCC. A training schedule has been developed and staff development has assigned children's training to staff who need the hours. The EVV system has had a soft launch and is being implemented. IPOS training continues to be missed. Additional training has been conducted at Leadership Meetings and PNOQMC. The children's team has been educated on how to run reports on the training hours within Relias.
Security Risk Assessment	Annual	Completed August 2025	Bay-Arenac Behavioral Health (BABH), in accordance with 45 CFR Part 160 and Part 164, must complete a HIPAA Risk Assessment to ensure all electronic protected health information (ePHI) created, received, maintained, or transmitted by a covered entity is adequately protected. This BABH security risk assessment process utilizes the Security Risk Assessment (SRA) tool provided by the United States Department of Health and Human Services. The SRA tool lists 126 security assessment questions, provides several different response choices to each question, and ways in which to comply when a non-compliant response is selected. BABH is compliant with 121 of the 126 questions within the DHHS SRA tool. Remediation plan is being addressed in this upcoming year. The 2026 SRA is being completed now.

Question Type	Questions	Compliant Answers	Compliance %
Required	94	90	96%
Addressable	32	31	97%
Total	126	121	96%

EDUCATION		
Persons Served	**Frequency**	**Status**
Consumer Council-Bay Consumer Council-Arenac	Annual/ PRN	Website contains Fraud Abuse and Privacy education. Consumer Council was educated on 09/24/2025 and 10/01/2025.
Self-Determination	As Needed	Self Determination education for new consumers has begun to be tracked and reported to MSHN as well as the 5% EOB's that are sent out annually.
Board of Directors	**Frequency**	**Status**
Full Board Corporate Compliance training	Annual	Completed June 2026

Additional compliance information provided for Board of Directors:

Date	Audience	Topic
5/7/2026	CCC Board Members	CC Semi Annual Plan, Annual Litigation Report, CC Plan, Dashboards for Privacy and Fraud, OIG work plan.

EDUCATION

5/7/2026	CCC Board Members	CC Dashboard, MSHN MEV Findings, Quarterly Fraud and Abuse report for FY26Q1 and FY26Q2.

Supervisors	Frequency	Status
Standing compliance agenda item on Bi-Weekly Leadership meetings	Monthly	Completed
Supervisor-specific corporate compliance training	Annual	Developed initial training and provided training via email to Supervisors.

Additional Educational Activities for Supervisors:

Date	Audience	Topic	Type
None			

Employees	Frequency	Status
New employee orientation to corporate compliance, privacy and confidentiality	Monthly	Completed every month.
Corporate compliance training	Annual	Completed 06/2026 – Annually for all employees during Staff Development Days
Privacy/security/confidentiality training	Annual	Completed 06/2026 – Annually for all employees during Staff Development Days
Corporate Compliance Plan in-service	Annual	2026 Corporate Compliance Plan 03/03/2026
Email security drills (by Security Officer)	Quarterly	Being completed monthly to quarterly last completed June 2026.

Additional Educational Activities for Personnel:

Date	Audience	Topic	Type
01/08/2026	PNOQMC – Primary Providers	Documentation requirements for Medicaid, BABHA Contract, and BABHA Policy and Recoupment Requirements	In-Person

Contracted Service Providers	Frequency	Status
Corporate Compliance Training for Residential/ Community Living Support Providers	Annual	Competed 4/30/2026
Corporate Compliance Training for Vocational Providers	Annual	Completed 09/2025
Corporate Compliance Training for Primary Providers	Annual	Completed 11/2025
Corporate Compliance Training for Autism Providers	Annual	Completed 4/30/2026

Additional Educational Activities for Contracted Service Providers:

Date	Audience	Topic	Type

Corporate Compliance Staff & Leadership	Frequency	Status
Review of Regulatory Changes	Monthly	In process
Review of Medicaid and General Fund Contract Boilerplate and Attachments	Yearly	In process
Review of CMS Office of Inspector General [Regulatory Compliance] Work Plan	Yearly	In process

Educational activities for compliance leadership:

Date	Audience	Topics	Type
04/15/2026	Melissa Prusi	Turning Medicare Audit Results into Smarter AuditsArtificial Intelligence	Webinar
04/28/2026	Melissa Prusi	2025 HIPAA Breaches & Fines: What Went Wrong and Your 2026 Action Plan	Webinar
04/29/2026	Melissa Prusi	Your Guide to Beating 2026's Phishing Epidemic	Webinar
05/13/2026	Melissa Prusi	Improving Outcomes Conference	In-Person
05/19/2026	Melissa Prusi	H.R.1 Eligibility Redeterminations: New Requirements, Timeline and Recommendations	Webinar
06/08/2026	Melissa Prusi	CMHA Summer Conference	In-Person
07/23/2026	Melissa Prusi	Medicaid and the Road Ahead: Spending Cuts, Work Requirements and What's Next for States, Providers and Families	Webinar

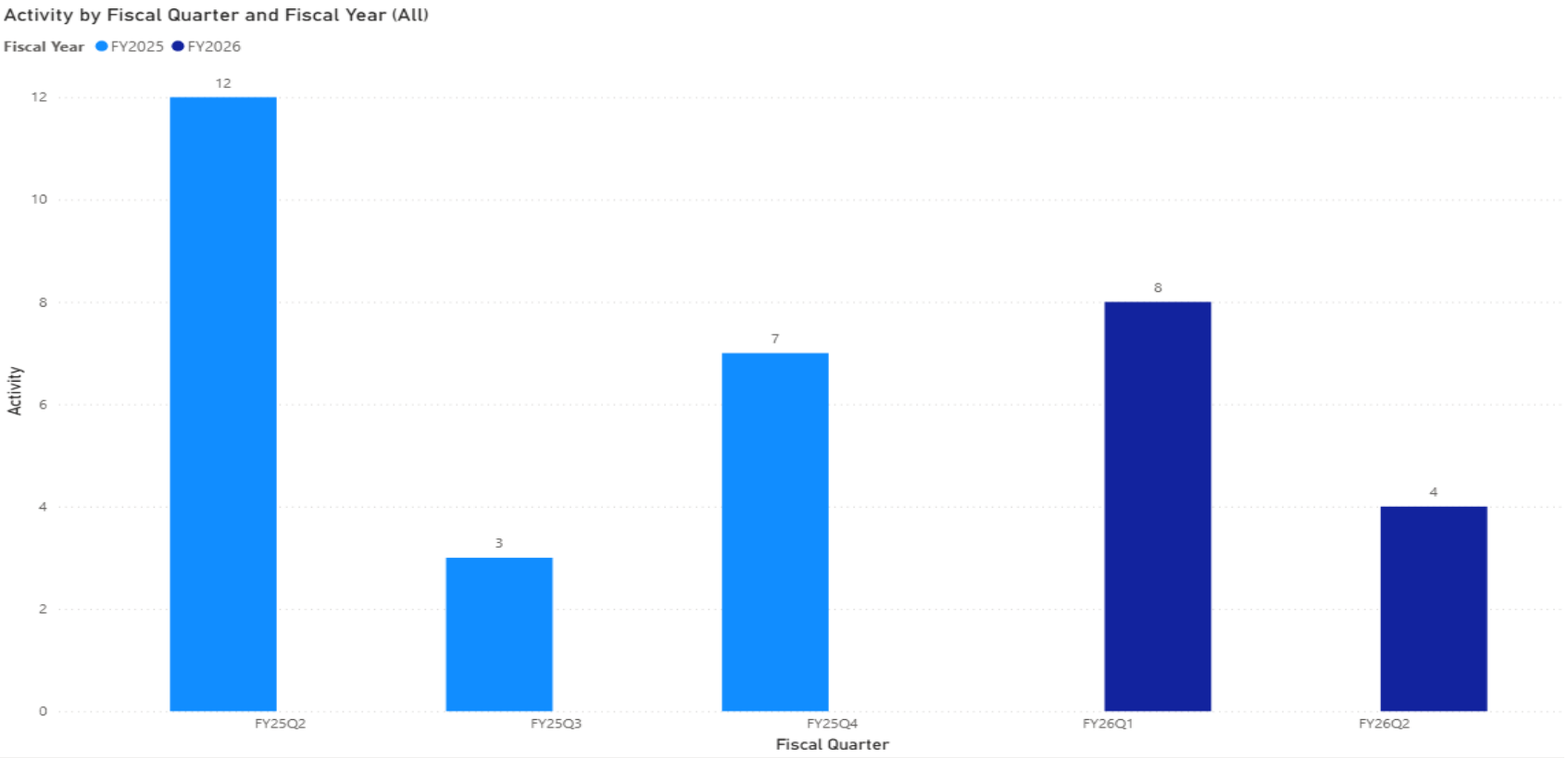
Report Prepared by:
Melissa Prusi, LBSW, MHSL
Director of Healthcare Accountability

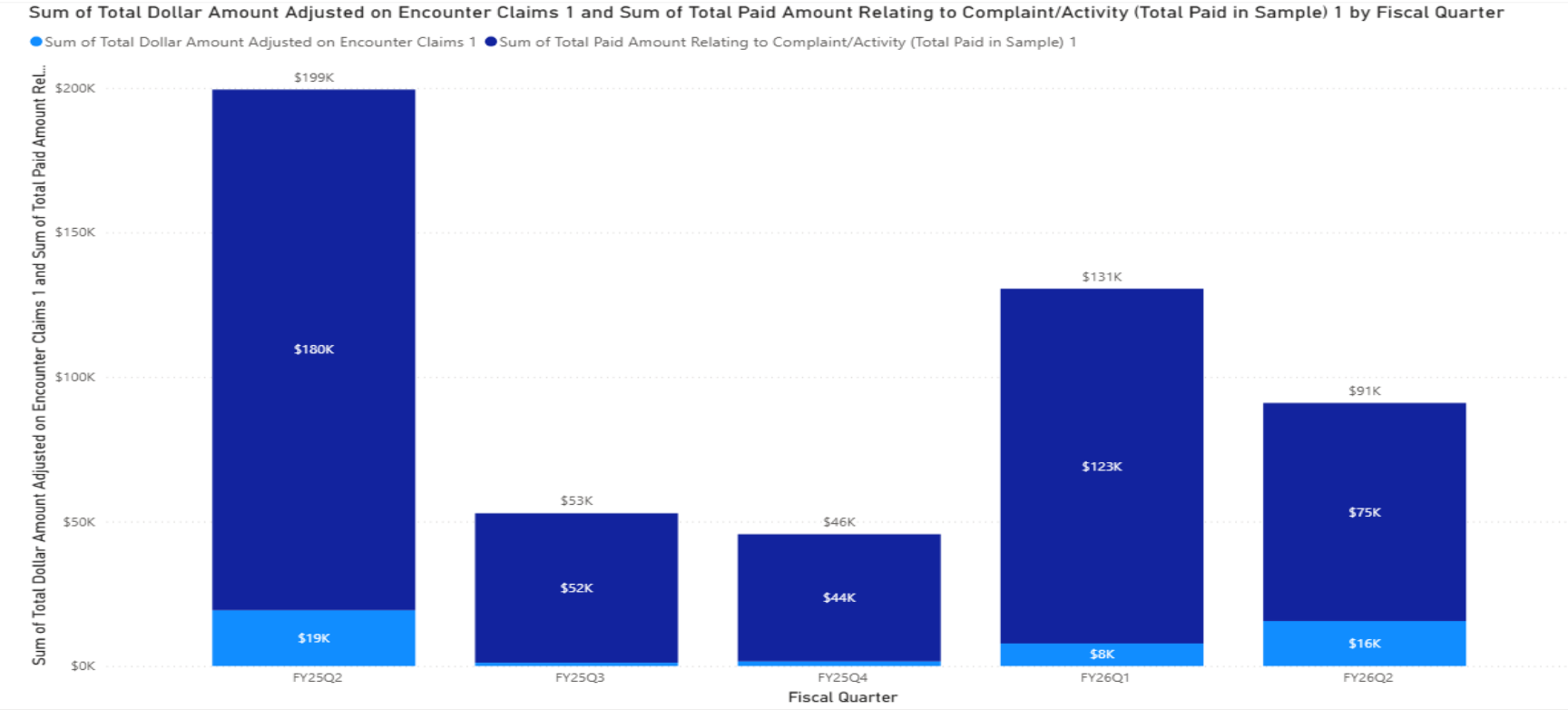
Date: July 22, 2026

Corporate Compliance Dashboard

Quarterly Fraud & Abuse Report – Healthicity Data

08/03/2026





Medicaid Encounter Validation (MEV) Site Review Summary

BABHA continues to conduct Medicaid Encounter Validation (MEV) site reviews of both direct service programs and contracted providers to verify that services billed to Medicaid are supported by appropriate clinical documentation and meet Medicaid requirements. Review findings identified a small percentage of claims requiring adjustment when compared to the total value of services reviewed each quarter. The majority of services examined were adequately documented and supported for reimbursement, demonstrating overall compliance with Medicaid billing and documentation standards.

Corrective actions and claim adjustments are implemented when necessary to address identified documentation deficiencies, support provider education, and strengthen ongoing compliance efforts. These reviews remain an important component of BABHA's Corporate Compliance Program and help ensure the integrity, accuracy, and accountability of Medicaid-funded services.

Key Takeaway: MEV reviews continue to demonstrate strong overall compliance among both direct and contracted providers, with identified issues representing a relatively small portion of reviewed claims and serving as opportunities for continuous quality improvement.

Executive Summary: Information Management Strategic & Operational Plan (2025–2026)

Purpose and Scope

The Information Management Strategic and Operational Plan outlines how BABHA will leverage technology and information systems to support its mission as a Community Mental Health Services Program (CMHSP). The plan guides decision-making related to technology investments, vendor relationships, security, and compliance while aligning with organizational priorities.

Strategic Direction

The plan includes long-term core strategies (3–5 years), environmental scan and risk analysis (1–2 years), and breakthrough initiatives (12–24 months). Planning is led by the Strategic Leadership Team and reviewed annually by the Board.

Key Strategic Priorities

- Maintain secure and reliable infrastructure
- Strengthen cybersecurity and risk management
- Improve data accessibility and reduce duplication
- Support remote work and telehealth
- Enhance staff training and system utilization
- Improve monitoring and user satisfaction

Key Strategic Initiatives & Risks

High priority areas include website accessibility compliance, cybersecurity risk mitigation, cloud cost management, business continuity planning, remote work security, workforce training to lower human element risks, and vendor management.

Key Financial Highlights

- IT Equipment Replacement Investment: Approximately $137,847 – subject to change based on bulk-pricing
- Cloud Computing Environment: Approx. $28,780/month (~$345,000 annually)
- Additional Costs: Telecommunications, software licensing, and vendor-hosted systems
- Financial Risks: Increasing cloud and vendor costs, redundant data storage, and underutilized licenses
- Cost Control Strategies: Vendor review, license optimization, standardized data storage, and cost-effective cloud solutions

Key Takeaways for the Board

BABHA maintains a strong, largely compliant IT infrastructure but faces growing financial pressure from cloud and vendor costs. Key risks include website accessibility compliance, cybersecurity vulnerabilities, and vendor management.

Recommended Board Focus Areas

1. Approve and oversee website accessibility strategy
2. Monitor cloud and vendor cost management
3. Support cybersecurity investments and training
4. Promote efficient and equitable technology access

06/24/2026

BAY ARENAC

BEHAVIORAL HEALTH

~~2024~~2025-~~2025~~2026

Information Management Strategic and Operational Plan

Updated by IS ~~Manager~~Department: ~~November 8, 2024~~ June 5, 2026

Strategic Leadership Team Approval: ~~November 12, 2024~~ June 16, 2026

Full Board Approval Date

~~2024~~2025-~~2025~~ 2026 Information Management Strategic and Operational Plan

Table of Contents

~~2024~~2025-~~2025~~ 2026 Information Management Strategic and Operational Plan

Scope

The Bay-Arenac Behavioral Health Authority (BABHA) Information Management Strategic and Operational Plan encompasses the organization's responsibilities as a Community Mental Health Services Program (CMHSP).

Overview

This document presents the BABHA Information Management Strategic and Operational Plan, specifically, the values and core strategies of the organization relative to information management and technologies, in support of the organization accomplishing its mission. It documents Leadership's current assessment of any forces in the environment with the potential to impact the organization's technological environment and defines strategies for responding. The Plan informs decision making in the use of technology and information management services, thereby influencing vendor relationships, service agreements, and so on. It also captures some operational processes to ensure these activities receive adequate attention on an annual basis to ensure quality and maintenance of technical edge.

Methodology

Information Management Strategic Planning for BABHA as an entity is performed by the Chief Executive Officer (CEO), members of the Strategic Leadership Team (SLT) ~~and~~, and the Information Systems ~~Manager~~Department. The SLT encompasses key leadership positions in the organization including the Chief Financial Officer, Director of Healthcare Accountability, Director of Integrated Care – ~~Primary Care, Director of Integrated Care - Specialty Care~~Acute Services; Long Term Services; Children & Families; Arenac Center, and the Director of Human Resources.

The BABHA Information Management Strategic Plan is comprised of the following components:

- Values and Guiding Philosophies, which define the extent to which the organization plans to utilize information technologies and information management tools to manage its operations.

- Core ~~Strategies~~Strategies, which are statements of long-term strategies (3-5 years) intended to facilitate organizational achievement of its mission, consistent with the aforementioned values.

- An Environmental Scan to identify opportunities and threats in the environment that may impact BABHA's ability to achieve its core strategies in the present or near future (1-2 years), including current research and technological advances.

- Breakthrough Initiatives: present short-term strategies (12-24 months) to address the highest priority environmental opportunities and threats, taking into consideration the organization's strengths and weaknesses. The strategies are specific with responsible parties, sub-tasks, and due dates defined.

Strategic initiatives by their nature do not include operational activities and are transformative in nature. The focus is on opportunities and threats with the potential to impact achievement of core strategies. Top priority is given to mission critical strategic opportunities and threats, with secondary priority given to systems transformation. Not every opportunity or threat warrants action by BABHA.

This document is reviewed by the Strategic Leadership Team (SLT) and the Board of Directors on an annual basis. In addition, the SLT engages in ongoing monitoring of the environment for opportunities and threats and report such information at the SLT meetings as warranted.

~~2024~~2025-~~2025~~ 2026 Information Management Strategic and Operational Plan

Values/Guiding Philosophies

1. Information technologies will effectively and efficiently support information capture and accessibility.
2. Information management practices will operate consistent with regulatory and contractual requirements and BABHA business rules.
3. Redundant data entry and reporting will be minimized. Information will be readily accessible to users.
4. Technologies and information management processes will enhance not hinder staff productivity and support optimal workflows.
5. Information security technology will be deployed to protect confidential information being stored, processed, or transmitted by the organization.
6. Technologies and information management will provide support for accessibility to IT systems for any authorized system user as defined by the agency.
7. Balance will be maintained between technological investment and benefit to the organization.
8. Information technology and information management vendors will operate in a manner that is consistent with the mission of BABHA, relative to their scope of work on behalf of BABHA.
9. Unless otherwise justified, selection of information technologies and information management tools will be consistent with commonly accepted standards and current best practices.
10. Staff will be trained and expected to take full advantage of current technology.
11. ~~BABHA will comply with product licensing requirements.~~
12. ~~12.~~11. Information technologies will be sensitive to the needs of stakeholders with less technological capacity and flexible enough to interact effectively.
13. ~~13.~~12. Collaborative decision-making will be used unless circumstances dictate otherwise.
14. ~~14.~~13. A base of knowledge will be maintained to ensure well-informed decisions are made.

~~2024~~2025-~~2025~~ 2026 Information Management Strategic and Operational Plan

Core Strategies

1. Maintain an optimal network capacity through proper management procedures and planned purchasing of bandwidth and other network services.
2. Maintain adequate server capacity through proper management procedures and proactively monitoring resource utilization.
3. Minimize e-storage demands on technological systems through appropriate information management (retention) practices.
4. Ensure ~~proper~~ system and network redundancies are implemented and tested on a regular basis as documented in the working business continuity and disaster recovery plan.
5. Control the risk and cost of change through use of test environments, fallback plans, request tracking and project management. ~~Quality controls utilized for all vendor projects.~~
6. Maintain ~~proper~~ equipment and product licensing inventories. Maintain a planned replacement schedule.
7. Provide periodic review of all system security software and measures including but not limited to anti-virus, firewalls, intrusion detection, encryption, and security policies and privacy practices as defined in policies C09-S03-T13 Security Awareness - Protection from Malicious Software and C09-S03-T14 Security Awareness - Log-in Monitoring, ~~-~~C09-S05-T10 – Videoconferencing recording transcribing and use of AI~~AI policies - add~~
8. Maintain telepresence and video conferencing capability.
9. Use technology to support remote access by community-based and remote BABHA staff.
10. In-house information systems subject matter expert(s) to maintain knowledge through ~~subscription~~ online ~~journals and print research~~ materials. Provide access to formal continuing education, and other training resources as warranted.
11. Flexible and focused training options for staff regarding information management and technologies.
12. Establish and maintain central repositories of data files and reports.
13. In-house subject matter expert(s) to maintain awareness of front-line user needs and workflows to ensure information management systems are meeting business demands.
14. ~~-~~Structured evaluation of user satisfaction and system performance using standardized tools, analytics, and qualitative feedback.~~Periodic and systematic assessment of user overall satisfaction using a standardized tool.~~

BAY ARENAC
BEHAVIORAL HEALTH

Environmental Scan, Analysis of Strengths, Weaknesses, Opportunities and Threats, and Breakthrough Initiatives

SECTION DESCRIPTION

BABH reviews what is occurring in the environment external to the organization and engages in an analysis and action planning process to ensure the organization continues to remain viable in order to achieve its mission.

An ENVIRONMENTAL SCAN identifies OPPORTUNITIES AND THREATS in the environment that may impact the organization's ability to achieve its core strategies in the present or near future (1-2 years). The organization defines opportunities and threats as follows:

Opportunities:	Conditions external to the organization that the organization may want to take advantage of in order to facilitate achievement of core objectives
Threats:	Conditions external to the organization that may hinder achievement of core objectives if not decreased or eliminated

Organizational STRENGTHS AND WEAKNESSES are then assessed for the highest priority opportunities and threats. The organization defines these terms as follows:

Strengths:	Attributes of the organization that are expected to be helpful to the organization in taking advantage of an opportunity or fending off a threat
Weaknesses:	Attributes of the organization that may hinder the organization's ability to take advantage of an opportunity or fend off a threat

BREAKTHROUGH INITIATIVES, present short-term strategies (12-24 months) to address the highest priority environmental opportunities and threats, taking into consideration the organization's strengths and weaknesses. The strategies are specific with responsible parties, sub-tasks, and due dates defined.

KEY: EDI=Electronic Data Interchange; EHR=Electronic Health Record; IS=Information Systems; LAN=Local Area Network; NSO=NetSource One; O365=Office 365; PCE=Peter Chang Enterprises; PRI=Primary Rate Interface; SLA=Service Level Agreement; SLT=Senior Leadership Team; VDI=Virtual Desktop Infrastructure; VPN=Virtual Private Network; WAN=Wide Area Network

Environmental Scan: HEALTH INFORMATION EXCHANGE

Lead Team Member: IS ~~Manager~~Department **Status:** Revised for ~~2024~~2025-~~2025~~2026

Impact on Ability to Accomplish Mission:

- Improve health care quality and patient outcomes by ensuring everyone involved in care has access to the same information
- Exchanging health information via an HIE or Direct Address messaging are core objectives of meaningful use

Opportunities or Threats:

Opportunities

- Exchanging information electronically will increase efficiency and reduce errors for BABH and the providers we exchange PHI with
- This will increase the amount of data in our system that is actual data instead of an image or page of data that cannot be tabulated and analyzed
- Eliminate dual entry for those agencies we exchange information with

Threats

- ~~None identified.~~ – Ssecurity risks, changing external staff passwords, we may not be familiar with staff calling or emailing to change password. Utilizing MFA to reduce risk

Strengths and Weaknesses (Response to Opps/Threats):

Strengths

- Our Electronic Health Record (EHR) has established connections and proven technologies to connect with an HIE
- The Healthcare Integration Steering Committee will direct meaningful HIE engagement

Weaknesses

- Many of our providers are accustomed to the traditional methods of exchanging PHI, i.e. fax, scan to email, etc.

Commented [MP1]: Mel to look into HISC and potential replacement

Commented [MP2R1]: This workgroup has been put on hold for now according to Joelin Hahn

Breakthrough Initiatives:	Target:	Resources:
1. Continue to build upon ~~Mi Gateway and VPR~~MiHIN health information exchange (HIE) solutions to exchange information with the primary health care and hospital communities.		IS ~~Manager; Director of Health Care Accountability; I.S. Help Desk/EHR Administrator, Medical Records Associate, Clinical Services Program Manager, Nursing Manager~~Department
2. Use direct address to exchange information that we routinely exchange PHI with, if/when other health care providers have direct messaging capability.	Ongoing	IS ~~Manager, I.S. Help Desk/EHR Administrator, Medical Records Associate, Clinical Services Program Manager, Nursing Manager~~Department

Environmental Scan: MANAGEMENT OF COMPUTING RESOURCES

Lead Team Member: IS ~~Manager~~Department **Status:** Revised for ~~2024~~2025-~~2025~~2026

Impact on Ability to Accomplish Mission:

- ~~The cloud computing environment recurring costs are directly related to the amount of resources used by the organization. (This is not accurate. It is the amount reserved).~~ Recurring costs within the Azure cloud computing environment are determined by the volume and configuration of resources reserved and maintained by the organization.
- Establishing document management practices can control use of computing resources and assist with establishing and enforcing document retention guidelines

Opportunities or Threats:

Opportunities

- Cloud computing environment is tightly integrated environment that can provide opportunities for more centralization and control of organizational records
- The ~~Office~~ MS 365 ~~(O365)~~ environment, including SharePoint, has a comprehensive data retention system that could be utilized to apply retention schedules to a variety of data elements held by the organization

Threats

- Cost of cloud computing environment will continually increase without management and monitoring of computing resources
- Under-reserving may affect performance or scalability.
- Document retention guidelines are difficult to enforce without negatively impacting user experience and functionality, i.e. email archiving
- Vendors increasing their licensing prices
- Possible loss of local vendor support
- ~~Some resources can generate costs in a non-transparent manner~~

Strengths and Weaknesses (Response to Opps/Threats)**:**

Strengths

- Cloud computing infrastructure is tightly integrated and more easily allows for centralized management and monitoring of computing resources
- Costs are predictable but fixed.
- Implementation of single G: drive improves ability for users to share documents
- Team has been identified to assist departments and users with the management of organizational records

Weaknesses

- Access to cloud storage data can be affected by speed of internet access
- Potential for interrupted access to cloud infrastructure
- ~~Agency maintains~~There ~~large amounts of~~is duplicative data that is not~~n't~~ necessary to keep and ~~poses~~pose security risks
- Reserving additional capacity increases monthly costs, even if usage fluctuates.

Breakthrough Initiatives:	**Target**	**Resources:**
1. Current cloud environment allows organization to consider leveraging less expensive ~~O~~MS365 cloud storage options where practical and applicable	Ongoing	IS ~~Manager, Director of Health Care Accountability, Senior Systems Administrator, I.S. Help Desk/EHR Administrator, IS Help Desk Specialist, Senior Programmer/ Analyst~~Department
2. Work with departments and users to establish unified data storage practices	Ongoing	IS ~~Manager, Senior Systems Administrator, I.S. Help Desk/EHR Administrator~~Department

3.	~~Migrate seldom-used data to secure cloud storage where practical and applicable~~	~~Ongoing~~	~~IS Manager, Senior Systems Administrator, Senior Programmer/ Analyst~~
4.	Move computing resources to Azure to save cost increase reliability and reduce complexity of the environment.	Ongoing	IS Department
5.	Obtain and evaluate at least three vendor proposals for major computing investments, ensuring cost efficiency, market alignment, and a secure, reliable computing environment that supports business continuity.	Ongoing	IS Department

Environmental Scan: BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN AND TESTING

Lead Team Member: IS ~~Manager~~Department **Status:** Revised for ~~2024~~2025-~~2025~~2026

Impact on Ability to Accomplish Mission:

- The organization's ability to function at an acceptable capacity when a disaster occurs is diminished without an updated plan and disaster recovery configuration
- Routine testing and documentation of that testing will ensure the functionality of the disaster recovery plan and all its components

Opportunities or Threats:

Opportunities

- Routine testing of the disaster recovery plan will ensure functionality and uncover any potential changes that could affect disaster operations
- ~~MiTel phone system is a distributed model with site-to-site fail-over capabilities by decentralizing infrastructure via distributed model~~
- Ring Central system is able to bring the phone system to staff wherever they have an internet connection

Threats

- ~~All critical network circuits terminate at NetSource One (NSO) creating single point of failure.~~ A failure of the Ring Central system would result in reduced or unavailable phone functionality, directly impacting Help Desk operations and Emergency Access Services (EAS)
- A Verizon service outage could render organizational Wi-Fi hotspots unavailable, negatively impacting business operations and staff workflow

Strengths and Weaknesses (Response to Opps/Threats)**:**

Strengths

- Network connections to agency sites have high throughput and redundant connections with both AT&T ~~ASE~~ circuits and Charter ~~VPN~~ connections; includes both voice and data network traffic
- UTM firewalls provide SD-WAN technology which allows for both the primary and backup network connections to be active and handle prioritized network traffic
- Offsite disaster recovery computing location is restored and tested quarterly~~.~~
- Data backups are tested monthly via routine data restores.
- The Electronic Health Record (EHR) system is hosted by the vendor, Peter Chang Enterprises (PCE), which has a redundant data center that is utilized and tested semi-annually
- Basic network connection is used by staff however when there is a power outage or Wi-Fi failure staff have Wi-Fi hotspots are available to EAS staff to ensure continuity for our crisis line and Emergency/Access services

Weaknesses

- Planning and testing for smaller component outages still must be accounted for, i.e. fiber optic failure at Mulholland
- Disaster recovery processes of outside vendors needs to be verified

Breakthrough Initiatives:	Target	Resources:
1. Continue to enhance testing procedures, documentation, and functionality of the business continuity and disaster recovery plan, as practical and applicable.	Ongoing	IS ~~Manager~~Department, ~~Senior Systems Administrator~~
2. BABHA will explore alternative communication methods and established outage procedures to	Ongoing	IS Department

support continuity of Help Desk and Emergency After-Hours Services (EAS) during Ring Central service disruptions.			
~~1.~~3. BABHA's business continuity and security risk assessments will assess hotspot usage, vendor performance, and available redundancy options to ensure continuity of essential work processes during service interruptions.	Ongoing	IS Department	

Environmental Scan: ~~MAINTAIN COST EFFECTIVE TELECOMMUNICATIONS SYSTEMS~~ IMPROVE BABHA'S WEBSITE AND ENSURE PATIENT PORTAL PROVIDES EQUAL ACCESS TO DIGITAL CONTENT BY ENHANCEMENT OR REDESIGN

Lead Team Member: ~~IS Manager~~ IS Department **Status:** Revised for ~~2024~~2025-~~2025~~2026

Impact on Ability to Accomplish Mission:

- ~~Maintaining efficient and cost-effective telecommunications systems will provide quality service while making additional resources available for the organizational mission.~~ Ensuring BABHA complies with Section 504 of the Rehabilitation Act which requires organizations receiving federal financial assistance—including schools, hospitals, and social service agencies—to provide equal access to digital content, such as websites, apps, and online programs, for individuals with disabilities. (Compliance generally mandates adhering to WCAG 2.1 Level AA standards. Digital Standards require that web content must be perceivable, operable, understandable, and robust (POUR principles)
- Ensuring that BABHA's online content and systems are current by assigning each section of the website to be maintained by the appropriate parties

Opportunities or Threats:

Opportunities:

- ~~Ensures that organization is not overpaying for outdated or underperforming services.~~ Explore website designers to determine if the current website can be updated or requires total redesign which can allow for a more user-friendly website

Strengths and Weaknesses (Response to Opps/Threats)**:**

Strengths:

- ~~The TelNet rates are very inexpensive compared to the previous carrier rates.~~ BABHA has the ability to choose a new webdesigner should this be necessary
- ~~Agency has redundant internet access at all our primary facilities that would allow for conversion to cloud-based telephone service~~ BABHA's Strategic Leadership Team

- Ensures the organization's website and other digital content remains an accurate reflection of current practices, services, and programs
- Can move to cloud based telephone service to improve reliability and increase access to phone system to remote and field workers Ensures the organization's website and other digital content complies with Section 504 of the Rehabilitation Act

Threats:

- TelNet services are inexpensive, but organization voice services with a single vendor represents single point of failure
- Non-compliance can lead to federal investigations (OCR), loss of funding (CMS/HHS), and private lawsuits.
- Current phone system will be end of life December 2025.

determined they will maintain responsibility to review the website contents on a scheduled basis

Weaknesses:

- TelNet outages illustrated that relying on local carriers to route calls introduces additional points of failure.
- BABHA'S website has outdated information which is not updated regularly
- BABHA's website does not meet these accessibility requirements

Breakthrough Initiatives:	**Target**	**Resources:**
1. Develop a cost-effective long-term telecommunications strategy that aligns with business initiatives and anticipated organizational needs in the context of the new hybrid office and remote work environment – i.e., reduced reliance on desk top phones, etc. Explore webdesign options to determine how best to improve BABHA's website and comply with Section 504 of the Rehabilitation Act	09/30/2026	Director of Health Care Accountability, IS Manager IS Department
2. Review BABHA's online content, assign each section of the website to appropriate parties to be reviewed/updated	09/30/2026	IS Department
3. Collaborate with PCE to ensure BABHA's patient portal complies with Section 504 of the Rehabilitation Act	09/30/2026 12/31/25	IS Department
1.4. Review BAAs to ensure accessibility requirements are met by vendors.	09/30/2026	IS Manager, Senior Systems Administrator, I.S. Help Desk/EHR Administrator IS Department and legal counsel
Implement RingCentral (or similar) cloud-based unified communications solution to replace our EOL phone system.		

Environmental Scan: IMPROVE SYSTEM SECURITY PRACTICES AND TECHNOLOGY

Lead Team Member: IS ManagerDepartment **Status:** Revised for 2025-20252026

Impact on Ability to Accomplish Mission:

- Improve security practices that govern system audits, security reviews, and documentation

Opportunities or Threats:

Opportunities

- Continue to use KnowBe4 Hook Security email phishing campaigns and user training

Threats

- Email phishing threats represent the greatest risk to organizational data

Strengths and Weaknesses (Response to Opps/Threats)**:**

Strengths

- Cloud environment is tightly integrated and newer technologies making auditing easier
- EHR has powerful system activity auditing tools
- Hosting provider is considered HIPAA-compliant datacenter provider
- MFA deployed to staff for VDI Office MS 365 services, and EHR access
- MFA deployed to providers that utilize BABHA EHR

Weaknesses

- The human factor is ~~still~~ a weak link in our security

Breakthrough Initiatives:	**Target**	**Resources:**
1. Explore~~Provide~~ in person training options for security threats	09/30/2026	IS Department
~~1.~~2. Continue end user education on security threats, especially with ~~KnowBe4~~ Hook phishing campaigns and individual training as necessary.	Ongoing	IS ~~Manager, Senior Systems Administrator, I.S. Help Desk/EHR Administrator, IS Help Desk Specialist~~Department
3. Add targeted training for high ~~-~~risk groups (Finance, IT, HR)	09/30/2026	IS Department

Environmental Scan: ~~INCREASE MOBILE AND REMOTE WORK TECHNOLOGIES~~STREAMLINE MOBILE AND REMOTE WORK TECHNOLOGIES

Lead Team Member: IS ~~Manager~~Department **Status:** Revised for ~~2024~~2025-~~2025~~2026

Impact on Ability to Accomplish Mission:

- ~~Improve remote collaboration tool capacity to allow for all staff to conduct secure virtual meetings with both internal and external parties~~
- Ensure staff have equipment that provides effective use of agency's remote work software tools
- Increase use of cloud services allowing ~~for~~ staff to securely access organizational data more easily when working remotely or in the community

Opportunities or Threats: **Strengths and Weaknesses** (Response to Opps/Threats)**:**

Opportunities

- Increase use of Microsoft Teams throughout agency. All staff with an agency email account are already licensed for the software via MS~~O~~365 subscription
- Broad deployment of iPads, laptops~~, Chromebooks~~, and agency cell phones allow staff to utilize commonly deployed virtual collaboration tools such as Microsoft Teams~~, Zoom,~~ and Doxy.me
- Increase use of cloud services securely allow for staff to access organizational data more easily when working remotely or in the community
- Have select staff pilot new cost-effective technologies to use in the community and remotely to ensure staff have the most efficient technology available

Threats

- Remotely managing a large fleet of devices can be challenging for the IS Department as control is decentralized from the company network to staff's home network
- Staff sometimes have limited or poor internet options when working remotely
- Risk of staff printing or storing documents that contains PHI in non-secure locations. Personal computers, cell phones, cloud or personal paper files at home.
- Risk of staff holding tele-sessions in an unsecure environment

Strengths

- Current ~~Office~~ MS 365 software subscriptions provide users with access to collaboration tools without additional cost
- Mobile equipment currently deployed to staff allows for remote work and collaboration
- All agency cell phones have an unlimited voice, text, and data service plan allowing for extended remote work at no additional cost

Weaknesses

- ~~Newly deployed thin clients are now capable of processing audio and video but do not have microphones or cameras limiting participation in virtual meetings from the office~~
- Keeping collaboration tools such as Microsoft Teams ~~and Zoom~~ updated on mobile devices can be challenging
- ~~All agency cell phone plans have unlimited hotspot data plans, however, data throttling begins after 10 gigabytes of usage~~
- Ability to monitor productivity of staff working remotely is available, but reports made available for supervisors could be improved.

Breakthrough Initiatives:	**Target**	**Resources:**
~~1.~~		
~~2. Implement the change to Microsoft 365 licenses from Office 365 licenses for additional management and security features, allowing for the IT Department to effectively manage the de-centralized nature of SharePoint.~~	~~02/15/25~~	~~Director of Health Care Accountability~~~~Senior Systems Administrator~~~~I.S. Help Desk/EHR Administrator~~
1. ~~Test~~ Explore SharePoint permissions and features to ensure permissions are appropriate for use based on employees need and "need to know" ~~online (Share point has been online for years..)~~ and OneDrive on a per-department basis	09/30/~~25~~26	IS ~~Manager~~Department, ~~Senior Systems Administrator~~
2. Explore Teams Channel permissions and features to ensure permissions are appropriate for use based on employees need and "need to know". a. IS Department to become proficient in the use and structure of SharePoint and Teams Channels b. IS Department to provide training for piloting end users then conduct training prior to pilot groups transitioning c. Pilot work groups, committees, or departments to ensure permissions support workflow and processes then move forward with transitioning as deemed appropriate.		IS Department~~IS Manager, Director of Health Care Accountability, Senior Systems Administrator, I.S. Help Desk/EHR Administrator~~
~~3.~~		
3. ~~Need action to complete this ...~~Explore options for monitoring of staff productivity with leadership	09/30/2026	IS Department
4. Identify and Address Barriers Keeping Staff on Zoom	09/30/2026	IS Department

Environmental Scan: INCREASE TECHNICAL TRAINING OFFERED TO STAFF

Lead Team Member: IS ~~Manager~~Department **Status:** Revised ~~2024~~2025-~~2025~~2026

Impact on Ability to Accomplish Mission:

- Additional technical training will allow staff to more efficiently use the technologies provided to them by the agency
- Effective remote work relies heavily on technology

Opportunities or Threats:

Opportunities

- The agency has numerous software tools staff might find beneficial with an enhanced knowledge of how they operate
- The IS Departmen~~'~~t can provide training both virtually and in person
- Relias training may have valuable training~~s~~ modules that could be offered to staff

Threats

- Lack of knowledge can hinder productivity or increase reluctance to use available technology

Strengths and Weaknesses (Response to Opps/Threats)**:**

Strengths

- IS Department staff are eager to provide training to staff on tools most commonly referred to the Help Desk
- Relias training library is extensive and easily deployed to staff
- Staff generally know how to use current common technology
- Staff reach out to the help desk if they have questions on how to use technology
- Staff are trained every time a new technology is implemented

Weaknesses

- Lack of staff participation with voluntary trainings offered
- Staff do not engage in additional training due to training overload
- Need to identify if and where staff knowledge gaps exist and what training would be both useful and appreciated.

Breakthrough Initiatives:	**Target**	**Resources:**
1. Provide users software tips and training opportunities through electronic means as a more efficient alternative to recommending more mandatory annual training	09/30/~~25~~26	IS ~~Manager~~Department ~~, Senior Systems Administrator, I.S. Help Desk/EHR Administrator, Senior Programmer~~/ ~~Analyst, LAN / Database Specialist, IS Help Desk Specialist~~ IS Department ~~IS Manager, Senior Systems~~ IS Department ~~Administrator, I.S. Help Desk/EHR Administrator, Senior Programmer/ Analyst, LAN / Database Specialist, IS Help Desk Specialist~~
2. ~~Investigate a wiki-style location on intranet/SharePoint for organizing and accessing past tips~~Provide training in multiple formats to staff, Tech Tips, videos, lunch and learns	~~09/30/25~~26 09/30/26	
3. Explore and identify staff member knowledge gaps exist and offer training options to address gaps	09/30/2026	
a. Explore ways to gauge staff member knowledge gaps and preferred training subjects		

~~2.~~

~~Provide training in multilemultiple formats to staff, tech tip Tuesdays, videos~~

~~1.~~

~~I.S. Help Desk/EHR AdministratorIS Help Desk SpecialistSenior Systems AdministratorSenior Programmer/ AnalystLAN / Database Specialist~~

Operational Initiatives

Environmental Scan: VENDOR MANAGEMENT AND PERFORMANCE MONITORING

Lead Team Member: IS ~~Manager~~Department **Status:** Revised for ~~2024~~2025-~~2025~~2026

Impact on Ability to Accomplish Mission:

- Ensure that vendor is providing acceptable levels of service and adhering to Service Level Agreement (SLA) parameters

Opportunities or Threats:

Opportunities

- ~~External monitoring of EHR, external VDI portal, telecommunication systems, and BABHA website uptime provides independent view of system availability~~BABHA's vendors monitor our VDI and EHR environments and provides consistent performance and responds quickly to address issues which allows the BABHA IT staff to concentrate on agency initiatives.

Threats

- Using vendors who lease or subcontract with larger vendors can make troubleshooting service issues more difficult
- Vendor consolidation and growth risk when an existing vendor is acquired by a larger organization or experiences significant growth in its client base may impact service quality, responsiveness, or consistency

Strengths and Weaknesses (Response to Opps/Threats)**:**

Strengths

- Users are quick to report issues to the helpdesk~~,~~ and ~~outage reports can be~~is tracked ~~in a SharePoint list~~through the help desk ticketing system ~~,~~and is accessible to all IT staff to collaborate on.

Weaknesses

- Too reliant on vendor to report performance problems with their services
- Lack of diversity in vendors can impact operations when experiencing service disruptions from a particular vendor
- ~~Old reporting tool "What's Up Gold" did not provide adequate insight into actual outages, instead only reporting if the IP address of the service responded to a ping, which resulted in many false positives, and false negatives.~~

Breakthrough Initiatives:	**Resources:**
~~1. Compare outage calculations against SLA parameters or other performance guidelines to ensure vendor compliance~~	~~IS Manager~~
~~2. Provide performance data for Leadership Dashboard reporting~~ ~~○ Wide and local area network issues~~ ~~○ Telepresence issues~~ ~~○ Cloud computing and Virtual Desktop Infrastructure (VDI) issues~~ ~~○ Phone issues~~ ~~○ Phoenix issues~~	~~IS Manager, Director of Health Care Accountability, I.S. Help Desk/EHR Administrator~~
~~3.~~ ~~Generate power BI reports for leadership dashboard from outage SharePoint list.~~ ~~This has been completed~~	~~IS Manager, LAN / Database Specialist, Senior Programmer/ Analyst~~
1. Audit use of staff software and application subscriptions (such as Zoom, Doxy, Adobe and Microsoft products) on a routine basis and adjust vendor agreements where feasible to eliminate unnecessary costs.	09/30/2026 IS ~~Manager~~Department, ~~LAN / Database Specialist, Senior Systems Administrator, Senior Programmer / Analyst,~~

2. Monitor vendor performance, customer service levels, and contractual compliance	~~I.S. Help Desk/EHR Administrator, IS Help Desk Specialist~~ 09/30/2026 IS Department
~~4.~~3. Explore other vendor options and seek out quotes from vendors to ensure BABHA vendors are cost-effective	01/31/2027 IS Department

Operational Initiative: CONTINUED DEVELOPMENT OF STANDARDIZED COMMUNICATIONS KNOWLEDGE

Lead Team Member: IS ~~Manager~~Department **Status:** Revised for ~~2024~~2025-~~2025~~2026

Impact on Ability to Accomplish Mission:

- In-depth knowledge of the various Electronic Data Interchange (EDI) formats utilized by the state, regional entities, and other healthcare data repositories will help BABHA facilitate the timely exchange of data with other organizations

Operational Actions:	Resources:
1. Continue developing institutional knowledge of file structures used for state encounter reporting, BH-TEDS/Mental Health Client-Level Data (MH-CLD) submissions, and new state consumer registry file	IS ~~Manager~~Department~~, Senior Programmer/ Analyst, I.S. Help Desk/EHR Administrator~~
2. Research American National Standards Institute (ANSI) -accredited standards within the healthcare industry such as HL7 International	IS ~~Manager~~Department, ~~Senior Programmer/ Analyst, I.S. Help Desk/EHR Administrator~~
3. ~~Research HIE vendors and the EHR Direct Messaging capabilities identifying potential uses for BABH~~	~~IS Manager, Senior Programmer/ Analyst, I.S. Help Desk/EHR Administrator, Medical Records Associate~~

Environmental Scan: INFORMATION SYSTEMS DOCUMENTATION

Lead Team Member: IS ~~Manager~~Department **Status:** Revised for ~~2024~~2025-~~2025~~2026

Impact on Ability to Accomplish Mission:

- Document information systems procedures, processes, and system designs to ensure adequate knowledge transfer and long-term functionality of department and systems

Opportunities or Threats:	**Strengths and Weaknesses** (Response to Opps/Threats)**:**
Opportunities • Create central repository for documentation • Cross-training within department will make documentation essential to success **Threats** • Lack of documentation limits knowledge transfer • Limits ability for cross training to be effective	**Strengths** • Tools necessary to capture and share knowledge are currently available • Data Governance Committee creates workgroup venue to standardize data driven project documentation • Standard documentation procedures have been established for report/data centric projects. **Weaknesses** • Programming and software development still needs a structured documentation process. • Need to finalize Quality Control protocols for system development, design, modifications, validations and documentation

Breakthrough Initiatives:	**Resources:**
1. ~~Establish standard documentation practices for information systems processes, procedures, and system design~~	~~IS Manager, Senior Systems Administrator, Senior Programmer/ Analyst, I.S. Help Desk/EHR Administrator, LAN / Database Specialist, IS Help Desk Specialist~~
2. Continue to develop documented standards of organizational data definitions and business processes	~~Director of Health Care Accountability,~~ IS ~~Manager~~Department~~, Quality Manager, Senior Programmer/ Analyst, LAN / Database Specialist~~
3. Investigate use of Microsoft Dev Ops for all source code to ensure access if lead staff not available	~~Senior Programmer/ Analyst, LAN / Database Specialist~~IS Department
4. Explore use Microsoft Share Point to standardize documentation processes to ensure continuity	IS ~~Manager~~Department, ~~I.S. Help Desk/EHR Administrator, Senior Programmer/ Analyst, LAN / Database Specialist~~
~~4.~~5. Prepare education plan and timelines for implementation to ensure agency permissions remain consistent and appropriate for use	IS Department

Environmental Scan: CONTINUE TO IMPROVE ANNUAL RISK ASSESSMENT PROCESS

Lead Team Member: IS ~~Manager~~Department **Status:** Revised for ~~2024~~2025-~~2025~~2026

Impact on Ability to Accomplish Mission:

- Continue to enhance tool to monitor risk, compliance, security, and the effectiveness of the organization's policies and procedures
- Identify gaps in compliance and security that can be used to drive the continuous improvement process

Opportunities or Threats:

Opportunities

- Can build upon internally conducted risk assessment with the new Security Risk Assessment tool released by the U.S. Department of Health and Human Services
- Evaluate physical security at all locations for possible improvements related to the protection of PHI

Threats

- Regular monitoring of risk is essential to maintaining compliance and a strong security posture
- Without an updated risk assessment, it is difficult to provide a gap analysis of risk, compliance, and security
- Proposed changes to the HIPAA Security Rule that have not yet been finalized and published could require significant effort to comply with changes.

Strengths and Weaknesses (Response to Opps/Threats)**:**

Strengths

- ~~2024~~ 2025 risk assessment can be used as a building block for broader inspections of security
- Tightly integrated cloud computing environment should limit number of technical anomalies reported

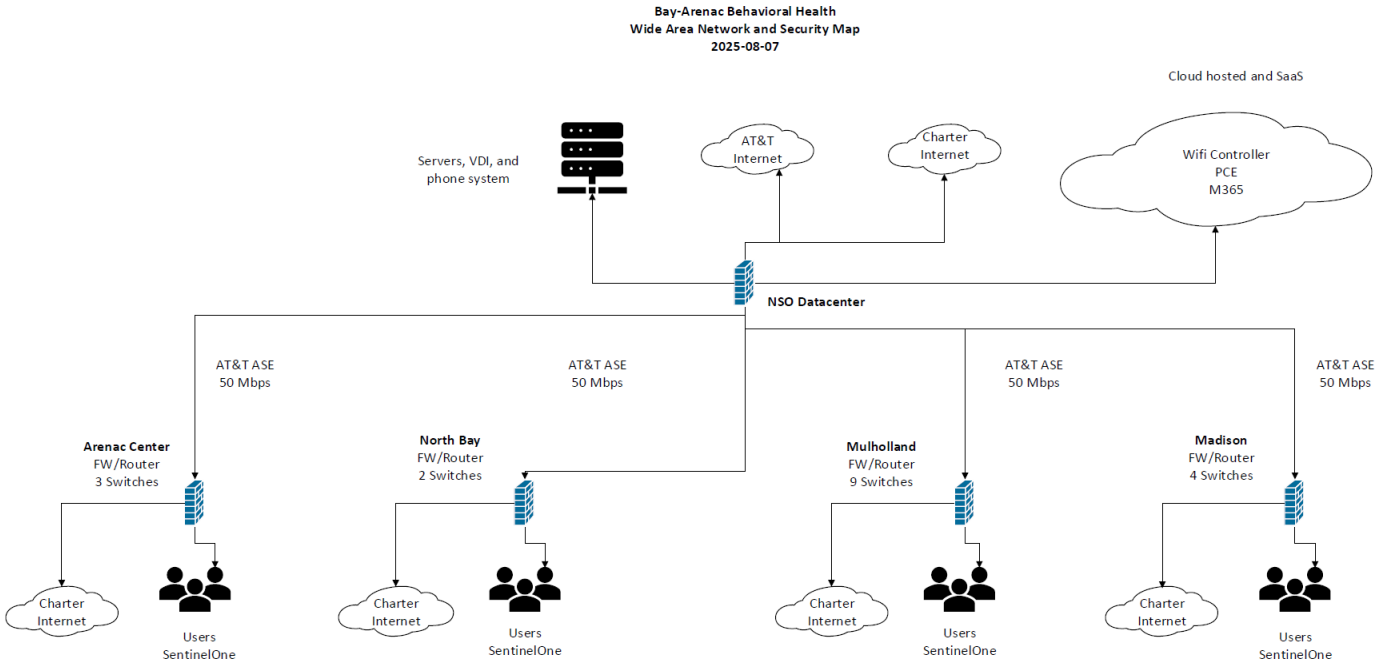
Weaknesses

- Continued development of disaster recovery plan testing and documentation
- The physical security at some locations could be improved as it relates to the protection of PHI
- Unable to monitor security of PHI in employees' remote work locations

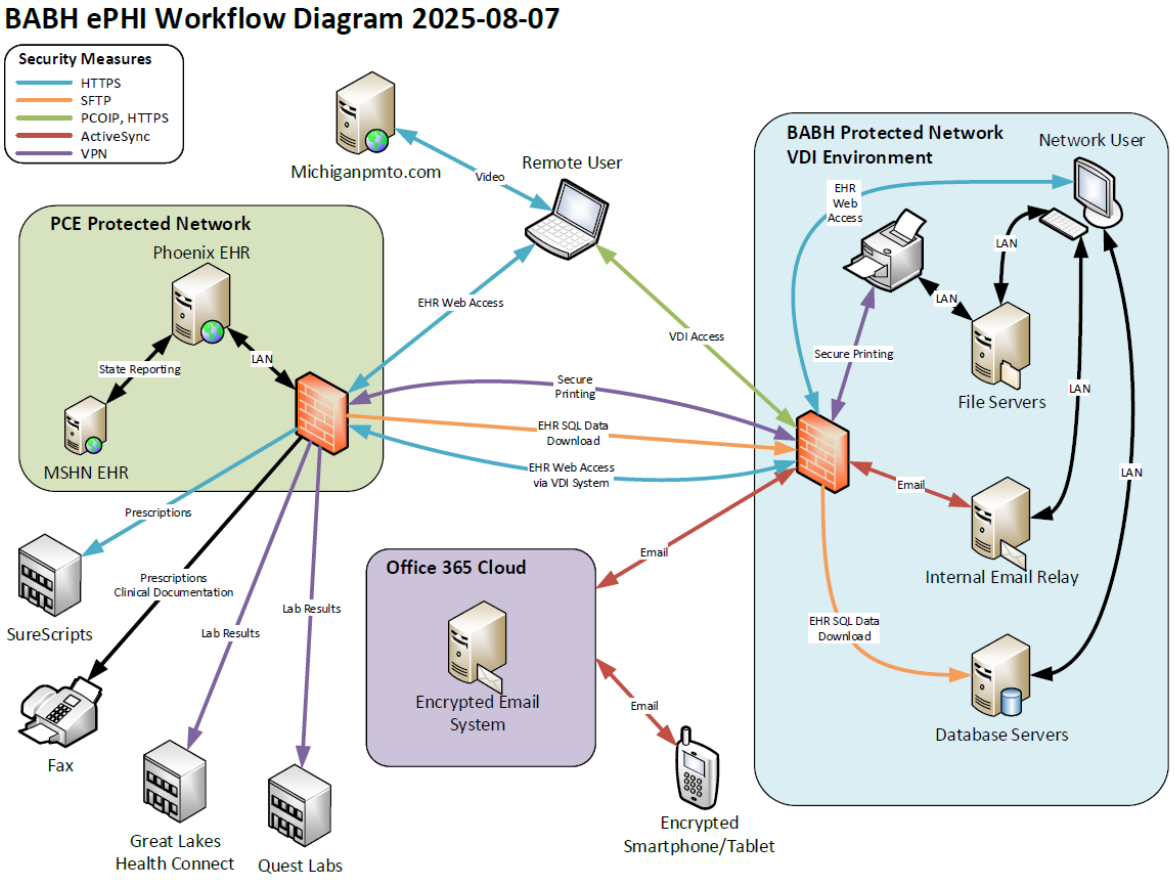
Breakthrough Initiatives:	**Resources:**
1. Continued development of risk assessment monitoring tool	IS ~~Manager~~Department
2. Perform risk assessment for the organization annually	IS ~~Manager~~Department
3. Obtain external security risk assessment through independent party per industry standards	IS Department
4. Remediate gaps identified in the risk assessment annually ~~3.~~	IS ~~Manager~~Department~~, Senior Systems Administrator, Senior Programmer/ Analyst, I.S. Help Desk/EHR Administrator, LAN / Database Specialist, IS Help Desk Specialist~~

Attachments

Wide Area Network and Security Map



e-PHI Workflow Diagram



Security Risk Assessment Findings and Remediation Plan 2024

Bay Arenac Behavioral Health

Completed By: Jesse Bellinger, IT Manager/Security Officer
Date Completed: July 01, 2024

I. Overview

Bay Arenac Behavioral Health (BABH), in accordance with 45 CFR Part 160 and Part 164, must complete a HIPAA Risk Assessment to ensure all electronic protected health information (ePHI) created, received, maintained, or transmitted by a covered entity is adequately protected.

This BABH security risk assessment process utilizes the Security Risk Assessment (SRA) tool provided by the United States Department of Health and Human Services. The SRA tool lists 120 security assessment questions, provides several different response choices to each question, and ways in which to comply when a non-compliant response is selected.

This document includes a summary of the 7 sections within the SRA tool, a breakdown of compliance in each section, and a description of the areas where BABH was not in full compliance with the requirement.

II. Security Risk Assessment Findings

Section 1 – SRA Basics

This section focuses on basic information about our SRA, including if we have ever completed an SRA, how often we conduct an assessment, the processes used to complete one, and how the results are reported.

Results

Question Type	Questions	Compliant Answers	Compliance %
Required	9	9	100%
Addressable	1	1	100%
Total	10	10	100%

BABH is fully compliant within this section.

Section 2 – Security Policies

Section 2 concentrates on agency policies and procedures, risk management processes, document retention of our completed SRA materials, and the role of the Security Officer in managing risk.

Results

Question Type	Questions	Compliant Answers	Compliance %
Required	8	8	100%
Addressable	0	0	N/A
Total	8	8	100%

BABH is fully compliant within this section.

Section 3 – Security and Workforce

Section 3 concentrates on the security aspects of workforce members. The questions focus on security awareness training, employment screening procedures, system and application access processes, and the competence of the Security Officer. Protection from malicious software and monitoring of login attempts is also addressed in this section.

Results

Question Type	Questions	Compliant Answers	Compliance %
Required	12	12	100%
Addressable	7	7	100%
Total	19	19	100%

BABH is fully compliant within this section.

Section 4 – Security and Data

This section focuses on access to electronically protected health information (ePHI). The questions center around how users are granted access, how are users identified when accessing ePHI, is access appropriate, the use of encryption, automatic logoff from systems, and backups.

Results

Question Type	Questions	Compliant Answers	Compliance %
Required	17	16	94%
Addressable	10	10	100%
Total	27	26	96%

BABH is not compliant within this section. Below are the question(s) that are not in full compliance.

Question 23 (Required): How do you determine the means by which ePHI is accessed?

Answer: Applications which access ePHI are identified, evaluated, approved, and inventoried, but we do not manage which devices can access these applications (e.g. workforce members personal devices accessing a cloud-based EHR without first identifying and approving the device)

DHHS Guidance: Unsecured points could compromise data accessed through an otherwise secure application. Consider implementing a device management process to ensure security standards are in place for all points accessing ePHI. Assign a separate user account to each user in your organization. Train and regularly remind users that they must never share their passwords. Require each user to create an account password that is different from the ones used for personal internet or e-mail access (e.g., Gmail, Yahoo, Facebook). For devices that are accessed off site, leverage technologies that use multi-factor authentication (MFA) before permitting users to access data or applications on the device. Logins that use only a username and password are often compromised through phishing e-mails. Implement MFA authentication for the cloud-based systems that your organization uses to store or process sensitive data, such as EHRs. MFA mitigates the risk of access by unauthorized users.

Section 5 – Security and the Practice

Section 5 targets physical security of devices, facilities, and the data center. The questions concentrate on how facilities are protected from unauthorized access, how devices protected from theft and unauthorized access, and an inventory of all equipment that store, process, or access ePHI.

Results

Question Type	Questions	Compliant Answers	Compliance %
Required	12	12	100%
Addressable	12	11	92%
Total	24	23	96%

BABH is not compliant within this section. Below are the question(s) that are not in full compliance.

Question 10 (Addressable): How do you validate a person's access to your facility?

Answer: We do not have lists of authorized persons or controls in place to identify persons attempting to access the practice, grant access to authorized persons, or prevent access by unauthorized persons.

DHHS Guidance: Consider appropriate methods of validating access to your facility. Implement and document safeguards determined to be reasonable and appropriate. Always keep data and network closets locked. Grant access using badge readers rather than traditional key locks.

Section 6 – Security and Business Associates

This section concentrates on how business associates are handled, the terms within our Business Associate Agreements (BAA), and assurances of compliance of our business associates.

Results

Question Type	Questions	Compliant Answers	Compliance %
Required	13	12	92%
Addressable	0	0	N/A
Total	13	12	92%

BABH is not compliant within this section. Below are the question(s) that are not in full compliance.

Question 7 (Required): How do you maintain awareness of business associate security practices?

Answer: We rely on the language of our BAAs to ensure that Business Associates are securing ePHI.

DHHS Guidance: Consider monitoring, auditing, or obtaining information from business associates to ensure the security of ePHI and include language about this in BAAs.

Section 7 – Contingency Planning

The final section of the SRA emphasizes contingency planning and security incidents. The questions center around identifying, documenting, and testing security incidents and emergency situations.

Results

Question Type	Questions	Compliant Answers	Compliance %
Required	19	19	100%
Addressable	1	1	100%
Total	20	20	100%

BABH is fully compliant within this section.

III. Security Risk Assessment Findings Summary

SRA Results

BABH is compliant with 118 of the 121 questions within the DHHS SRA tool. The areas BABH will focus on in the coming year are improving facility access validation and managing devices that access ePHI.

Question Type	Questions	Compliant Answers	Compliance %
Required	90	88	98%
Addressable	31	30	97%
Total	121	118	97%

IV. Security Risk Assessment Remediation Plan

Section 4 – Security and Data

Question 23 (Required): How do you determine the means by which ePHI is accessed?

Answer: Applications which access ePHI are identified, evaluated, approved, and inventoried, but we do not manage which devices can access these applications (e.g. workforce members personal devices accessing a cloud-based EHR without first identifying and approving the device)

Remediation Plan: Available options to limit device access to the cloud based EHR include IP Filtering and/or a browser cookie. Due to BABH's use of contracted providers, both options present an unreasonable burden to both end users and IT staff.

Standard 164.312(d) "Person or Entity Authentication" is the referenced rule for Section 4, Question 23. This standard has no implementation specifications and requires a covered entity to "Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed".

Access to PHI via our EHR software is protected by username, password, and 2 factor authentication. This ensures the person seeking access is who they say they are by requiring them to combine something they have (the time sensitive 2FA code generated by the token or authenticator app) and something they know (their username and password).

Our current practice provides reasonable security without placing an unreasonable burden on end users and IT staff. It is therefore not reasonable for us to follow the guidance within the SRA tool in this case.

Section 5 – Security and the Practice

Question 10 (Addressable): How do you validate a person's access to your facility?

Answer: We do not have lists of authorized persons or controls in place to identify persons attempting to access the practice, grant access to authorized persons, or prevent access by unauthorized persons.

Remediation Plan: Access to most facilities is controlled except for Mulholland. A recent change at the Mulholland site caused the doors to be open to the public. Most sites have video monitoring to track attempts to access the facility, except for North Bay.

The Security Officer will work with the Senior Leadership Team and the Facility Manager on ways to improve monitoring unauthorized attempts to access our facilities, and work on reasonable measures to secure Mulholland.

Section 6 – Security and Business Associates

Question 7 (Required): How do you maintain awareness of business associate security practices?

Answer: We rely on the language of our BAAs to ensure that Business Associates are securing ePHI.

Remediation Plan: BABH will not be pursuing the DHHS Guidance within the DHHS SRA Tool. The hhs.gov website contradicts the guidance provided within the tool. The hhs.gov website explicitly states that covered entities are not required to monitor or oversee the means by which their business associates carry out privacy safeguards or the extent to which the business associate abides by the privacy requirements of the business associate agreement. Our current practice adheres to the guidance provided on hhs.gov website. (Reference: FAQ 236 Is a covered entity liable for, or required to monitor the actions its business associates? https://www.hhs.gov/hipaa/for-professionals/faq/236/covered-entity-liable-for-action/index.html)

Security Risk Assessment Findings and Remediation Plan 2025
Bay-Arenac Behavioral Health

Completed By: Jesse Bellinger, IT Manager/Security Officer
Date Completed: 08/06/2025

I. Overview

Bay-Arenac Behavioral Health (BABH), in accordance with 45 CFR Part 160 and Part 164, must complete a HIPAA Risk Assessment to ensure all electronic protected health information (ePHI) created, received, maintained, or transmitted by a covered entity is adequately protected.

This BABH security risk assessment process utilizes the Security Risk Assessment (SRA) tool provided by the United States Department of Health and Human Services. The SRA tool lists 126 security assessment questions, provides several different response choices to each question, and ways in which to comply when a non-compliant response is selected.

This document includes a summary of the 7 sections within the SRA tool, a breakdown of compliance in each section, and a description of the areas where BABH was not in full compliance with the requirement.

II. Security Risk Assessment Findings

Section 1 – SRA Basics

This section focuses on basic information about our SRA, including if we have ever completed an SRA, how often we conduct an assessment, the processes used to complete one, and how the results are reported.

Results

Question Type	Questions	Compliant Answers	Compliance %
Required	9	9	100%
Addressable	1	1	100%
Total	10	10	100%

BABH is fully compliant within this section.

Section 2 – Security Policies

Section 2 concentrates on agency policies and procedures, risk management processes, document retention of our completed SRA materials, and the role of the Security Officer in managing risk.

Results

Question Type	Questions	Compliant Answers	Compliance %
Required	8	8	100%
Addressable	0	0	N/A
Total	8	8	100%

BABH is fully compliant within this section.

Section 3 – Security and Workforce

Section 3 concentrates on the security aspects of workforce members. The questions focus on security awareness training, employment screening procedures, system and application access processes, and the competence of the

Security Officer. Protection from malicious software and monitoring of login attempts is also addressed in this section.

Results

Question Type	Questions	Compliant Answers	Compliance %
Required	11	11	100%
Addressable	8	8	100%
Total	19	19	100%

BABH is fully compliant within this section.

Section 4 – Security and Data

This section focuses on access to electronically protected health information (ePHI). The questions center around how users are granted access, how are users identified when accessing ePHI, is access appropriate, the use of encryption, automatic logoff from systems, and backups.

Results

Question Type	Questions	Compliant Answers	Compliance %
Required	20	19	95%
Addressable	10	10	100%
Total	30	29	96.7%

BABH is not compliant within this section. Below are the question(s) that are not in full compliance.

Question 23 (Required): How do you determine the means by which ePHI is accessed?

Answer: Applications which access ePHI are identified, evaluated, approved, and inventoried, but we do not manage which devices can access these applications (e.g. workforce members personal devices accessing a cloud-based EHR without first identifying and approving the device)

DHHS Guidance: Unsecured points could compromise data accessed through an otherwise secure application. Consider implementing a device management process to ensure security standards are in place for all points accessing ePHI. Assign a separate user account to each user in your organization. Train and regularly remind users that they must never share their passwords. Require each user to create an account password that is different from the ones used for personal internet or e-mail access (e.g., Gmail, Yahoo, Facebook). For devices that are accessed off site, leverage technologies that use multi-factor authentication (MFA) before permitting users to access data or applications on the device. Logins that use only a username and password are often compromised through phishing e-mails. Implement MFA authentication for the cloud-based systems that your organization uses to store or process sensitive data, such as EHRs. MFA mitigates the risk of access by unauthorized users.

Section 5 – Security and the Practice

Section 5 targets physical security of devices, facilities, and the data center. The questions concentrate on how facilities are protected from unauthorized access, how devices protected from theft and unauthorized access, and an inventory of all equipment that store, process, or access ePHI.

Results

Question Type	Questions	Compliant Answers	Compliance %
Required	12	12	100%
Addressable	12	11	92%
Total	24	23	96%

BABH is not compliant within this section. Below are the question(s) that are not in full compliance.

Question 10 (Addressable): How do you validate a person's access to your facility?

Answer: We do not have lists of authorized persons or controls in place to identify persons attempting to access the practice, grant access to authorized persons, or prevent access by unauthorized persons.

DHHS Guidance: Consider appropriate methods of validating access to your facility. Implement and document safeguards determined to be reasonable and appropriate. Always keep data and network closets locked. Grant access using badge readers rather than traditional key locks.

Section 6 – Security and Business Associates

This section concentrates on how business associates are handled, the terms within our Business Associate Agreements (BAA), and assurances of compliance of our business associates.

Results

Question Type	Questions	Compliant Answers	Compliance %
Required	15	12	80%
Addressable	0	0	N/A
Total	15	12	80%

BABH is not compliant within this section. Below are the question(s) that are not in full compliance.

Question 7 (Required): How do you maintain awareness of business associate security practices?

Answer: We rely on the language of our BAAs to ensure that Business Associates are securing ePHI.

DHHS Guidance: Consider monitoring, auditing, or obtaining information from business associates to ensure the security of ePHI and include language about this in BAAs.

Question 14 (Required): Does the organization require business associates and third-party vendors to implement security requirements more stringent than required in the HIPAA Rules?

Answer: No, contracts with vendors or BAs outline requirements to follow the HIPAA Rules as applicable to BAs without additional cybersecurity protocols.

DHHS Guidance: The HIPAA Rules require a covered entity to obtain satisfactory assurances from its business associate that it will appropriately safeguard PHI it receives or creates on behalf of the covered entity. Organizations could consider protocols within their business practice to include enhanced cybersecurity and supply chain requirements beyond those required by the HIPAA Rules that third parties can follow and how compliance with the

requirements may be verified. Rules and protocols for information sharing between the organization and suppliers are detailed and included in contracts between the two.

Question 15 (Required): How do you track and verify business associate and third-party vendor compliance to security policies and where are these policies documented?

Answer: The organization verifies business associate and third-party vendor status each year but does not perform evaluations.

DHHS Guidance: The organization could require business associates and third-party vendors to disclose cybersecurity features, functions, and known vulnerabilities of their products and services for the life of the product or the term of service. Contracts could require evidence of performing acceptable security practices through self-attestation, conformance to known standards, certifications, or inspections. Business associates and third-party vendors could be monitored to ensure they are fulfilling their security obligations throughout the relationship lifecycle.

Section 7 – Contingency Planning

The final section of the SRA emphasizes contingency planning and security incidents. The questions center around identifying, documenting, and testing security incidents and emergency situations.

Results

Question Type	Questions	Compliant Answers	Compliance %
Required	19	19	100%
Addressable	1	1	100%
Total	20	20	100%

BABH is fully compliant within this section.

III. Security Risk Assessment Findings Summary

SRA Results

BABH is compliant with 121 of the 126 questions within the DHHS SRA tool.

Question Type	Questions	Compliant Answers	Compliance %
Required	94	90	96%
Addressable	32	31	97%
Total	126	121	96%

IV. Security Risk Assessment Remediation Plan

Section 4 – Security and Data

Question 23 (Required): How do you determine the means by which ePHI is accessed?

Answer: Applications which access ePHI are identified, evaluated, approved, and inventoried, but we do not manage which devices can access these applications (e.g. workforce members personal devices accessing a cloud-based EHR without first identifying and approving the device)

Remediation Plan: Available options to limit device access to the cloud based EHR include IP Filtering and/or a browser cookie. Due to BABH's use of contracted providers, both options present an unreasonable burden to both end users and IT staff.

Standard 164.312(d) "Person or Entity Authentication" is the referenced rule for Section 4, Question 23. This standard has no implementation specifications and requires a covered entity to "Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed".

Access to PHI via our EHR software is protected by username, password, and 2 factor authentication. This ensures the person seeking access is who they say they are by requiring them to combine something they have (the time sensitive 2FA code generated by the token or authenticator app) and something they know (their username and password).

Our current practice provides reasonable security without placing an unreasonable burden on end users and IT staff. It is therefore not reasonable for us to follow the guidance within the SRA tool in this case.

Section 5 – Security and the Practice

Question 10 (Addressable): How do you validate a person's access to your facility?

Answer: We do not have lists of authorized persons or controls in place to identify persons attempting to access the practice, grant access to authorized persons, or prevent access by unauthorized persons.

Remediation Plan: Access to most facilities is controlled except for Mulholland second floor, which uses a shared hallway with Hospital staff; individual offices are able to be locked on that floor when not occupied. Most sites have video monitoring to track attempts to access the facility, except for North Bay, although a recent policy change requires the ability for consumers to opt out of being recorded, which creates a conflict between privacy and security.

The Security Officer will work with the Senior Leadership Team to navigate the conflict in privacy and security, and if necessary, recommend appropriate cameras to monitor access attempts.

Section 6 – Security and Business Associates

Question 7 (Required): How do you maintain awareness of business associate security practices?

Answer: We rely on the language of our BAAs to ensure that Business Associates are securing ePHI.

Remediation Plan: BABH will not be pursuing the DHHS Guidance within the DHHS SRA Tool. The hhs.gov website contradicts the guidance provided within the tool. The hhs.gov website explicitly states that covered entities are not required to monitor or oversee the means by which their business associates carry out privacy safeguards or the extent to which the business associate abides by the privacy requirements of the business associate agreement. Our current practice adheres to the guidance provided on hhs.gov website. (Reference: FAQ 236-Is a covered entity liable for, or required to monitor the actions its business associates? https://www.hhs.gov/hipaa/for-professionals/faq/236/covered-entity-liable-for-action/index.html)

Question 14 (Required): Does the organization require business associates and third-party vendors to implement security requirements more stringent than required in the HIPAA Rules?

Answer: No, contracts with vendors or BAs outline requirements to follow the HIPAA Rules as applicable to BAs without additional cybersecurity protocols.

Remediation Plan: We have language in our BAAs that BAs are to take "appropriate safeguards" to protect PHI in addition to compliance with the Security Rule and HITECH act. We do not necessarily require adherence to more stringent standards from our BAs than what is outlined in the HIPAA rules, but the language of our BAAs does not rule that out. The question referenced here does not refer to any current HIPAA regulation, but the proposed changes to the HIPAA security rule that have not yet been published may include this. The current language of this rule may make compliance challenging with large providers who only issue boilerplate BAAs and will not change their practices for individual customers. Smaller providers could face significant administrative challenges adhering to this standard as well. The Security Officer will work with SLT to evaluate question 14's impact, and what steps could be taken to prepare for potential rule changes, as well as evaluate if compliance with this question is currently feasible.

Question 15 (Required): How do you track and verify business associate and third-party vendor compliance to security policies and where are these policies documented?

Answer: The organization verifies business associate and third-party vendor status each year but does not perform evaluations.

Remediation Plan: This question appears to be related to question 14, both of which are new in the SRA for this year. Currently there is no HIPAA rule referenced that would require compliance with either question. Proposed changes to the Security rule that is currently NPRM status could likely impact this. The Security Officer will work with SLT to evaluate question 15's impact, and what steps could be taken to prepare for potential rule changes, as well as evaluate if compliance with this question is currently feasible.

Information Technology Equipment Replacement Schedule

Objective

The purpose of this information technology equipment replacement schedule is to outline a systematic plan for the replacement of the agency's oldest computer equipment ensuring efficient and effective management of BABH's budget and computing capabilities. This schedule will provide an equipment lifecycle strategy for all client technology deployed within the agency minimizing the negative aspects of using older information technology.

Older computing equipment is:

- slower at processing employee tasks reducing employee productivity
- more expensive to support
- less energy efficient
- prone to more security breaches

This equipment replacement schedule should be considered a general guide and can be adjusted year-to-year to accommodate other agency needs or budgetary constraints.

Schedule

Device Type	Replacement Schedule
Desktop Computers	Replace devices every 4 years
Standard Laptop Computers	Replace devices every 4 years
Chromebooks	Replace devices every 4 years
iPads/Tablets	Replace devices every 3 years
10ZiG Thin Clients	Replace devices every 6 years
Desktop Printers	Replace devices every 6 years
Computer Monitors	Replace devices every 8 years

Replacement Cost

Device Type	Quantity	Unit Cost*	Total Cost*
Chromebooks (swap w/ surface)	17	$1,500	$25,500
Laptop	57	$1,500	$85,500
Desktop	17	$1,500	$25,500
iPad	3	$449	$1347
Total			$137,847

*Costs subject to change based on market and bulk pricing

~~Device Type~~	~~Quantity~~	~~Unit Cost~~	~~Total Cost~~
~~Chromebooks (swap with Surface)~~	~~23~~	~~$800~~	~~$18,400~~
~~iPad~~	~~12~~	~~$450~~	~~$5,400~~
~~Laptop~~	~~19~~	~~$1,500~~	~~$28,500~~
~~*totals*~~	~~54~~	-	~~$52,300~~

Equipment Qualifying for Replacement in 2026~~5~~

Category	BABH Asset Tag	Purchased Date	Years Since Purchase	Manufacturer	Model Number	Assigned To
Laptop	1697	12/14/2016	10	Dell	Latitude E5550	Alexandria Karas
Laptop	1699	12/15/2016	10	Dell	XPS 15	Kimberly Jinks
Laptop	8608	6/12/2020	6	Dell	XPS 15 7590	Kevin Motyka
Laptop	8165	9/10/2020	6	Dell	XPS 15	Deidra Walker
Laptop	8177	9/10/2020	6	Dell	XPS 15	Stacy Krazinski
Laptop	8208	9/30/2020	6	Dell	XPS 13	Sarah Holsinger
Laptop	8274	10/15/2020	6	Dell	XPS 13"	Jordan Wells
Laptop	8278	12/19/2020	6	Dell	XPS 15"	Jennifer Lasceski
Laptop	8280	12/20/2020	6	Dell	XPS 15"	Andrea Rayl
Laptop	8279	12/20/2020	6	Dell	XPS 15"	Bradley Parker
Laptop	1815	2/2/2021	5	Dell	XPS 15"	ES Dept
Laptop	1826	5/1/2021	5	Dell	XPS 15 9500	Irina Back
Laptop	1827	5/13/2021	5	Dell	XPS 15" 9500	Emily Gerhardt
Laptop	1828	5/20/2021	5	Dell	XPS 15" 9500	Stacy Krasinski
Laptop	1830	7/1/2021	5	Dell	XPS 15 9500	Dr. Movva
Laptop	1834	9/1/2021	5	Dell	XPS 15 9500	Lynn Meads
Laptop	8874	5/6/2022	4	Dell	xps 15	Pamela Vanwormer
Laptop	8861	5/12/2022	4	Microsoft	Surface Laptop Go 1943 i5	Kaitlyn Kokaly
Laptop	8873	5/12/2022	4	Dell	XPS 15	Flavia Devasconcelos
Laptop	1944	5/24/2022	4	Dell	XPS 15 9520	ES Dept
Laptop	8870	6/1/2022	4	Microsoft	Surface Go 1943	Eric Strode
Laptop	8872	6/15/2022	4	Microsoft	1493	Princess Hardy
Laptop	8881	7/25/2022	4	Dell	XPS15	Ashley Badour
Laptop	1905	7/27/2022	4	Lenovo	Thinkpad L15G3	Melissa Prusi
Laptop	8887	7/28/2022	4	Ms Surface	TNU-00001	Rebecca Leo
Laptop	1902	7/28/2022	4	Lenovo	Thinkpad L15G3	Amy Folsom
Laptop	8894	7/28/2022	4	Ms Surface	KC8-00001	Ashlee Grusnick
Laptop	1901	7/28/2022	4	Lenovo	Thinkpad L15G3	Tayla Stinson
Laptop	8916	7/28/2022	4	Ms Surface	2013	Karen Heinrich
Laptop	8899	7/28/2022	4	Ms Surface	KC8-00001	Alexus Smith
Laptop	8895	7/28/2022	4	Ms Surface	KC8-00001	Benjamin Tenney
Laptop	1904	7/28/2022	4	Lenovo	Thinkpad L15G3	Melissa Deuel
Laptop	1900	7/28/2022	4	Lenovo	Thinkpad L15G3	Christine Klatt
Laptop	1817	7/28/2022	4	Lenovo	Thinkpad L15G3	Johnelle Luther

Laptop	8878	7/28/2022	4	Lenovo	20YU001LUS	Meera Mohan
Laptop	1818	7/28/2022	4	Lenovo	Thinkpad L15G3	Kimberly Cereske
Laptop	1819	7/28/2022	4	Lenovo	Thinkpad L15G3	Tamera Matuszewski
Laptop	8897	7/28/2022	4	Ms Surface	KC8-00001	Rachel Lemiesz
Laptop	8885	7/28/2022	4	Ms Surface	TNU-00001	Kerensa Hecht
Laptop	8917	7/28/2022	4	Ms Surface	2013	Dustin Babcock
Laptop	8918	7/28/2022	4	Ms Surface	2013	Shaun Beyer
Laptop	8886	7/28/2022	4	Ms Surface	TNU-00001	Mariah Castillo
Laptop	8891	7/28/2022	4	Ms Surface	TNU-00001	Craig Kanicki
Laptop	8892	7/28/2022	4	Ms Surface	TNU-00001	Traci Lupcke
Laptop	1906	9/29/2022	4	Lenovo	Thinkpad L15 G3	Laurel McClure
Laptop	1907	10/13/2022	4	Lenovo	Thinkpad L15 G3	Marci Rozek
Laptop	8922	10/28/2022	4	Microsoft	2013	Joan Patten
Laptop	8927	11/18/2022	4	Microsoft	8QD-00023	ES Staff
Laptop	8933	11/18/2022	4	Microsoft	8QD-00023	Karen Lothian
Laptop	8926	11/18/2022	4	Microsoft	8QD-00023	Dean Deshaw
Laptop	8930	11/18/2022	4	Microsoft	8QD-00023	Lisa Mcalister
Laptop	8923	11/18/2022	4	Microsoft	8QD-00023	Melissa Reetz
Laptop	8925	11/18/2022	4	Microsoft	8QD-00023	Tonya Labelle
Laptop	8932	11/18/2022	4	Microsoft	8QD-00023	Meredith Bickel
Laptop	8963	11/22/2022	4	Microsoft	2013	Alexis Riley
Laptop	8934	12/22/2022	4	Microsoft Surface Go2 2013	8QD-00048	Susan Curtis
Laptop	1908	12/22/2022	4	Lenovo Thinkpad L15 G3	21C3004VUS	Jill Cederberg
Desktop	8006	8/15/2016	10	Dell	Optiplex 7040	Christopher Pinter
Desktop	6477	8/15/2016	10	Dell	Optiplex	Help desk
Desktop	8004	8/15/2016	10	Dell	Optiplex 7040	Brenda Beck
Desktop	6481	8/15/2016	10	Dell	Optiplex 7040	Tonia Wilczynski
Desktop	6485	8/15/2016	10	Dell	Optiplex 7040	Help desk
Desktop	6472	8/16/2016	10	Dell	Optiplex	Andrea Rayl
Desktop	8011	8/24/2017	9	Dell	Optiplex 5050	Finance
Desktop	6537	8/25/2017	9	Dell	Optiplex 5050	Help desk
Desktop	6535	8/25/2017	9	Dell	Optiplex 5050	Jill Cederberg
Desktop	6533	8/29/2017	9	Dell	Dell OptiPlex 5050 - SFF	Susan Curtis
Desktop	8104	10/16/2018	8	Dell	OptiPlex 7060	Help desk
Desktop	8102	10/22/2018	8	Dell	OptiPlex 7060	Denise Hartman
Desktop	6720	8/28/2019	7	Dell	Optiplex 3060	Help desk
Desktop	8747	7/1/2021	5	Dell	Optiplex 7090 Micro	Kathryn Brooks
Desktop	8880	8/1/2022	4	Dell	D15U	Room 210
Desktop	8882	8/1/2022	4	Dell	D15U	Room 113
Desktop	8879	8/1/2022	4	Dell	D15U	Roderick Smith
Chromebook	8647	7/1/2021	5	Acer	314	Arenac Kiosk
Chromebook	8642	7/1/2021	5	Acer	314	Susan Vian

Chromebook	8645	7/1/2021	5	Acer	314	Brian Kruzell
Chromebook	8632	7/1/2021	5	Acer	314	Amanda Christie
Chromebook	8658	7/1/2021	5	Acer	314	Ashley Aho
Chromebook	8663	7/1/2021	5	Acer	314	Bradley Parker
Chromebook	8621	7/1/2021	5	Acer	314	Jessica Kohn
Chromebook	8636	7/1/2021	5	Acer	314	Jodi Histed
Chromebook	8651	7/1/2021	5	Acer	314	Lori Lagalo
Chromebook	8664	7/1/2021	5	Acer	314	Maryssa Schneider
Chromebook	8643	7/1/2021	5	Acer	314	Stephanie Blaylock
Chromebook	8666	7/1/2021	5	Acer	314	Timothy Woodcock
Chromebook	8633	7/1/2021	5	Acer	314	Sarah Van Paris
Chromebook	8635	7/1/2021	5	Acer	314	Sarah Van Paris
Chromebook	8625	7/1/2021	5	Acer	314	Shalynda Rutherford
Chromebook	8624	7/1/2021	5	Acer	314	Casey Binkley
Chromebook	8653	7/1/2021	5	Acer	314	Jenna Mahar
iPad	8141	10/09/2019	7	Apple	6th Gen	Anne Sous
iPad	8281	01/03/2021	5	Apple	8th Gen 10.2"	Mickayla Miller
iPad	8292	01/04/2021	5	Apple	8th Gen 10.2"	Antonio Vega

~~OLD LIST – NEEDS TO BE REPLACED~~

~~Category~~	~~BABH Asset Tag~~	~~Purchased Date~~	~~Years Since Purchase~~	~~Manufacturer~~	~~Model Number~~	~~Signed out to~~
~~ChromeBook~~	~~8637~~	~~7/1/2021~~	~~3~~	~~Acer~~	~~314~~	~~Birdie Brown~~
~~ChromeBook~~	~~8656~~	~~7/1/2021~~	~~3~~	~~Acer~~	~~314~~	~~Lisa Husarick~~
~~ChromeBook~~	~~8653~~	~~7/1/2021~~	~~3~~	~~Acer~~	~~314~~	~~Jenna Mahar~~
~~ChromeBook~~	~~8651~~	~~7/1/2021~~	~~3~~	~~Acer~~	~~314~~	~~Lori Lagalo~~
~~ChromeBook~~	~~8647~~	~~7/1/2021~~	~~3~~	~~Acer~~	~~314~~	~~Allison Gruehr~~
~~ChromeBook~~	~~8645~~	~~7/1/2021~~	~~3~~	~~Acer~~	~~314~~	~~Brian Kruzell~~
~~ChromeBook~~	~~8643~~	~~7/1/2021~~	~~3~~	~~Acer~~	~~314~~	~~Stephanie Blaylock~~
~~ChromeBook~~	~~8642~~	~~7/1/2021~~	~~3~~	~~Acer~~	~~314~~	~~Susan Guertin~~
~~ChromeBook~~	~~8658~~	~~7/1/2021~~	~~3~~	~~Acer~~	~~314~~	~~Ashley Furtaw~~
~~ChromeBook~~	~~8638~~	~~7/1/2021~~	~~3~~	~~Acer~~	~~314~~	~~Andrea Rayl~~
~~ChromeBook~~	~~8636~~	~~7/1/2021~~	~~3~~	~~Acer~~	~~314~~	~~Jodi Histed~~
~~ChromeBook~~	~~8635~~	~~7/1/2021~~	~~3~~	~~Acer~~	~~314~~	~~Sarah VanParis~~
~~ChromeBook~~	~~8632~~	~~7/1/2021~~	~~3~~	~~Acer~~	~~314~~	~~Amanda Christie~~
~~ChromeBook~~	~~8629~~	~~7/1/2021~~	~~3~~	~~Acer~~	~~314~~	~~Monica Baniel~~
~~ChromeBook~~	~~8625~~	~~7/1/2021~~	~~3~~	~~Acer~~	~~314~~	~~Shalynda Rutherford~~
~~ChromeBook~~	~~8624~~	~~7/1/2021~~	~~3~~	~~Acer~~	~~314~~	~~Caseyt Birkley~~
~~ChromeBook~~	~~8621~~	~~7/1/2021~~	~~3~~	~~Acer~~	~~314~~	~~Jessica Hegenaver~~
~~ChromeBook~~	~~8620~~	~~7/1/2021~~	~~3~~	~~Acer~~	~~314~~	~~Kim Jinks~~
~~ChromeBook~~	~~8640~~	~~7/1/2021~~	~~3~~	~~Acer~~	~~314~~	~~Holli Vogel~~
~~ChromeBook~~	~~8663~~	~~7/1/2021~~	~~3~~	~~Acer~~	~~314~~	~~Brad Parker~~
~~ChromeBook~~	~~8633~~	~~7/1/2021~~	~~3~~	~~Acer~~	~~314~~	~~Sarah VanParis~~
~~ChromeBook~~	~~8664~~	~~7/1/2021~~	~~3~~	~~Acer~~	~~314~~	~~Maryssa Schneider~~
~~ChromeBook~~	~~8666~~	~~7/1/2021~~	~~3~~	~~Acer~~	~~314~~	~~Timothy Woodcock~~
~~iPad~~	~~8286~~	~~1/4/2021~~	~~3~~	~~Apple~~	~~8th Gen 10.2"~~	~~Timothy Woodcock~~
~~iPad~~	~~8275~~	~~9/13/2019~~	~~5~~	~~Apple~~	~~iPad 6th Generation~~	~~Nichole Sweet~~

iPad	6740	9/4/2019	5	Apple	6th Gen	Tracy Landrey
iPad	6735	11/1/2019	5	-	6th Gen	Anne Sous
iPad	6748	9/23/2019	5	-	6th Gen	Ellen Leskiak
iPad	6724	9/23/2019	5	-	6th Gen	Justin Louks
iPad	8140	10/9/2019	5	-	6th Gen	Anne Sous
iPad	8142	11/1/2019	5	-	6th Gen	Sara McRae
iPad	6734	11/1/2019	5	-	6th Gen	Theresa Adler
iPad	8149	11/6/2019	5	-	6th Gen	Audra Jungnitsch
iPad	8126	9/24/2019	5	apple	-	Melissa Haney
iPad	6521	5/17/2017	7	Apple	iPad Pro 12.9"	Kelly Bryan
Laptop	6026	10/15/2018	6	Dell	Latitude	Kelly Bryan
Laptop	1720	3/1/2017	7	Lenovo	Yoga 460	Lori Boucard
Laptop	6520	3/1/2017	7	Dell	Latitude 3460	Tina Dilley
Laptop	1728	8/25/2017	7	Dell	XPS 15	Viki Atkinson
Laptop	1717	3/1/2017	7	-	Yoga 460	Heather Nix
Laptop	1736	8/25/2017	7	Dell	XPS 13"	Nicholas Berkobien
Laptop	1735	8/25/2017	7	Dell	XPS 13"	Amber Wade
Laptop	1725	8/29/2017	7	Dell	XPS	Lisa Nagel
Laptop	1733	8/25/2017	7	Dell	XPS	Traci Hopper
Laptop	1746	8/25/2017	7	Dell	XPS 13	Recipient Rights
Laptop	1744	8/25/2017	7	Dell	XPS 13	Shaun Beyer
Laptop	1730	8/25/2017	7	Dell	XPS 15	Melanie Corrion
Laptop	1731	8/25/2017	7	Dell	XPS 15"	Marci Rozek
Laptop	1697	12/15/2016	8	Dell	Latitude E5550	Alexandria Karas
Laptop	1706	12/15/2016	8	Dell	XPS	Tina Dilley
Laptop	1695	12/12/2016	8	Dell	Latitude E5570	Teri Rosa
Laptop	1692	8/15/2016	8	Dell	Latitude E7270	Mariah Castillo
Laptop	1701	12/15/2016	8	Dell	XPS 15	Greg Lietzow
Laptop	6332	1/1/2015	9	Dell	Latitude E5550	Ann Nephews

BABH Master Agreement List

Item	Purpose	Notes	Licenses	Agreement	Invoice Only	Hosting/ Vendor	Term Start	Term End	Scope/Users	Fee/Rate	Annual Cost
NSO	Cloud computing environment (NSO-HOST-Web service was cancelled effective 10/31/2025 - $200/mo)	Monthly summary Iaas $10,875.75 Security $2954.60 Backups $2,195 Management $2,775.80 3rd party subs $9,979.20 Total monthly: $28,780.35	-	X	-	NSO	2/1/2023	2/1/2026	-	Autorenew on an annual basis	$345,336.20
BlueHost.com	Website Hosting and Support	-	-	-	-	BlueHost.com	04/23/2025	04/23/2028	-	- $359.64 for 36 mos	- 119.88 per year
-	-	-	-	-	-	-	-	-	-	-	-
Zoom	Telepsychiatry and conference room video conferencing	Month to month service used for telepsychiatry and video conferencing	X	-	-	Zoom	Month to Month	Month to Month	48 licenses - will reduce next year 1 Room Connectors	$14.29 per user per month $~~34.20~~ 49.00per H.232 Room Connector for external meetings	$735.09~~20.79~~ total/mo -
Verizon Wireless	for mobile phone service	Monthly access fees for service on 225 lines & equipment charts on 225 lines 224 lines 12/19/2025	-	-	-	-	-	-	-	-	-
Charter Acct 8245-12-	for general guest access at offices	-	-	-	-	Charter	-	evergreen	-	-	-

318-007-7655												
AT&T Internet-based VPN - direct fiber internet circuits - billed directly to BABHA from AT&T	Mulholland Building	AT&T Account Number: 989 R41-0200 612 2	-	X	-	AT&T	11/1/2025	Monthly	50 MBPS	4839.26/mo	$58,071.12/yr
- ASE Circuit (Ethernet) AT&T Internet-based VPN	Madison Building	AT&T Account Number: 989 R41-0125 619 9	-	X	-	AT&T	- 11/1/2025 - -	- - - -	50 MBPS	- - -	- - -
ASE Circuit AT&T Internet-based VPN	Arenac Building	ASE 20mb Circuit between Arenac and NSO Hampton Place location	-	X	-	AT&T	- 11/1/2025 - -	- - - Monthly	- 50 MPBS - -	- - -	- - -
- ASE Circuit (Ethernet)	Kawkawlin Site (North Bay)	AT&T Account Number: 989 R41-0229 718 4	-	X	-	AT&T	8/23/2018	Monthly	50 MBPS	-	-
Omnilert - Mass Notification System	Omnilert - mass notification system for alerting staff of emergent situations via email, SMS, and calling	Licensed for 325 Users. 250 staff contacts and 2 contacts for each provider.	1 annual license fee 325 user fee	x	-	Omnilert	9/28/2025	09/27/2026	325 users	Platform Cost $1,800/yr Annual user fee $4.20	1800 1365 $3165/ annual

	cell and desk phones										
Ruckus Wireless - NSO Trever Shetler at NSO indicated this is our corporate wireless solution - 12/30/2025 email	-	Support license renewals for controller and access point licenses; provides the latest patches and free warranty replacement if the device fails. This renewal is being done through Abadata at this time.	14	-	-	NSO/ Ruckus	6/3/2024	6/3/2027	-	- - - $170/month - - - -	- - - $2040/annual - - - -
*Fortinet (NSO) Firewall renewals (FortiAnalyzer end of life no longer billed $75/mo) but does include FortiGate (co-term renewal $9,090/year from 09/16/25 - 10/01/26) and FortiManager renewal ($245/year from 10/01/25 - 10/1/26)	-	Support for Fortinet UTM firewalls. Includes all branch firewalls and main FW at NSO network hub; support for Forti-Mgr and Forti-Analyzer servers; subscription for ongoing threat to keep security devices upgraded. Bought service with 5-year term when purchasing equipment.	-	x	-	NSO/ Fortinet	FortiGate $9090/yr FortiManager ($245/yr)	10/01/26 10/01/26	09/30/2031 09/30/2031	Prepaid 5 year term.	$9,090/yr & $245/yr

SSL Certificate - Wild Card Email noted - Standard Wildcard SSL Renewal connected to .babha.org	for multiple use *babha.org	Cost confirmed 03/16/2026 per email notification.				Go-Daddy	5/28/2026	05/27/2027	one multi-use cert	- $449.99	$499.99/yr
Domain Registration Account - babha.org	web domain for access to network for BABHA	Some domains are through Go-Daddy; others through Network Solutions			X			10/2030		Prepaid 5-year term $105.85	$105.85
Adobe allowed two users per license	Acrobat used to update PDF documents	BABH has 6 ~~5~~2 Adobe subscriptions - Acrobat– J. Louks, T Adler, S. McRae, B. Beck, M.Giesken (Annual), J. Sporman (annual)	X				Acrobat - May 2013	n/a	Acrobat – J. Louks, T Adler, S. McRae, B. Beck, M.Giesken (Annual), J. Sporman (annual)	Acrobat - $14.99/month/user	179.88 /user
DocuSign	eSignature	Handled by Finance directly Business Pro Edition - 5 licenses Premier Support - 1 annual license					4/20/2026	4/19/2027		$40/per month per license $360/year	$2400/yr $2730/yr ttl
			X				-	-			

Fixed Asset Software (Sage)	Finance - asset management	handled by Finance directly									
PCE Clinical Information Systems	EMR Implementation	IT does not handle this contract	-	-	-	-	-	-	-	-	-
PCE Clinical Information Systems	ASP Services	IT does not handle this contract	-	-	-	-	- - -	- - -	-	-	-
PCE Clinical Information Systems	EPCS	E-prescribing (including controlled substances) for 10 prescribers	X	-	-	-	~~1/16/2014~~	~~evergreen~~	~~10 licenses~~	~~$1,500/month per prescriber~~	~~$18,000.00~~
~~CAFAS (Functional Assessment Systems)~~	~~web service with Multi-Health Systems~~	~~to permit PCE- Phoenix integration w/ CAFAS/ PECAFAS~~	-	-	-	-	- -	- -	~~implementation fee & annual fee~~	~~$1,999 implementation fee~~ ~~$499 annual fee~~	~~$499/yr~~
SpeechExec-Pro Transcribe	Dictation software for Madison Clinic	-	-	-	-	-	#1 01/2026 #2 07/29/24	#1 01/2028 #2 07/29/26	Two licenses	#1 - $208.00/ two year subscription #2 - $293.00 / two-year subscription	$293.00/yr &$208.00 each $501 ttl annual
Jam Software – TreeSize Professional	program used to monitor/report file sizes, folders, folder permissions.	-	-	-	-	-	-	10/30/2026	1 license – T.Adler	$35.00/yr	$35.00
MSDN (Microsoft Developer	software development tools used by	Licenses have been established	X	-	-	Vendor varies	12/1/2025	12/1/2028	2 licenses - LNagel and GLietzow	$2601.38 for 3yr term	-

Commented [LN3]: @Greg Lietzow @Melissa Prusi Do we still have CAFAS?

Network) was through PC Connection; now CDW	Greg W and Greg L; Visual Studio is obtained through MSDN; (used for Gallery)	for both Lisa Nagel and Greg Lietzow				based on price						
Progress Software - was Telerik DevCraft Support and Maintenance	software development tools (used for Gallery)	Reduced from 2 to 1	X	X	-	-	2/27/2026	2/27/2027	1 license	-	$849.00	

Ring Central CX (EAS/HelpDesk) EX all	Professional Services (Fixed Fee) - Labor is quoted as a fixed-fee per statement of work - Any item not outlined in the statement of work is not included and therefore may be subject to additional pricing at our standard T&M rates on a separate ticket SubTotal $64,522.05 Monthly Recurring breakdown EX -	RingCX Implementation Package - REMOTE $22,500.00 Service Credits 3 - TTL - $25,239.50	EX 269 Tfree 84 CX 37 e911 269	x	-	Ring Central	7/15/2025	7/14/2028	EX 269 Tfree 84 CX 37 e911 269	3 yr term	-

	$44,048.00 Monthly Recurring breakdown CX - $42,180.00 Hardware Fees - $14,526.00										

Item	Purpose	Notes	Licenses	Agreement	Invoice Only	Hosting/ Vendor	Term Start	Term End	Scope/ Users	Fee/Rate	Annual Cost
-	-	-	-	-	-	-	-	-	-	-	-
NSO	Cloud computing environment	Monthly summary Iaas $10,875.75 Security $2954.60 Backups $2,195 Management $2,775.80 3rd party subs $9,979.20 Total monthly: $28,780.35	-	X	-	NSO	2/1/2023	2/1/2026	-	-	##########
BlueHost.com	Website Hosting and Support	-	-	-	-	Blue Host. com	4/23/2022	4/23/2025	-	$323.64 for 36m	$107.88 per year
-	-	-	-	-	-	-	-	-	-	-	-

Commented [GL4]: @Lisa Nagel - cost.. ? Backups?

Go To Meeting	Meeting services and audio conferencing service	Help Desk is admin - investigate reducing to 1 license	x	-	-	-	3/20/2014	evergreen	3 users	16.00/month/ seat	$576
OpenVoice Conf Rm # 7833212 Moderator PIN 8240193	conference calling service	T Adler Is administrator	x	-	-	-	-	-	3 users	.08 cents/per minute + ISF rate (usually around 20/25 percent)	-
Zoom	Telepsychiatry and conference room video conferencing	Month to month service used for telepsychiatry and video conferencing	x	-	-	Zoom	Month to Month	Month to Month	78 47users 1 Room Connectors	$14.99 per user per month $34.20$50 per H.232 Room Connector for external meetings	4718.28
Verizon Wireless	for mobile phone service	Monthly access fees for service on 225 lines & equipment charts on 225 lines	-	-	-	-	-	-	-	-	-
Communications as a Services (CaaS) - ShoreTel and BABH network equipment	Call center functionality and support for IP communicator	ES/Access Center call center and Help Desk phone systems	x	x	"	NSO	9/1/2017	9/1/2022	Phone System Network switches Network routers Fax system	1778.75 / mo	##########
Charter Acct 8245-12-318-007-7655	for general guest access at offices	-	-	-	-	Charter	-	evergreen	-	-	-

Commented [GL5]: @Lisa Nagel - this cost is higher right?

ASE Circuit (Ethernet)	Mulholland Building	AT&T Account Number: 989 R41 0200 612 2		X		NSO	8/23/2018	Monthly	50 MBPS	$752.64/mo 3/21	$9,031.68
ASE Circuit (Ethernet)	Madison Building	AT&T Account Number: 989 R41 0125 619 9		X		NSO	8/23/2018	Monthly	50 MBPS	$752.64/mo 3/21	$9,031.68
ASE Circuit	Arenac Building	ASE 20mb Circuit between Arenac and NSO Hampton Place location		X		NSO	8/23/2018	Monthly	50 MPBS	$752.64/mo 3/21	$9,031.68
ASE Circuit (Ethernet)	Wirt Building	AT&T Account Number: 989 R41 0068 081 1		X		NSO	8/23/2018	Monthly	50 MBPS	$752.64/mo 3/21	$9,031.68
ASE Circuit (Ethernet)	ASE Fiber Hub - NSO Hampton Place	ASE Hub req'd to provide a hub and spoke infrastructure for ASE Circuits being installed as of 8/23/18		X		NSO	8/23/2018	8/23/2021	250 MBPS	$1257.57/mo 3/21	##########
ASE Circuit (Ethernet)	Kawkawlin Site (North Bay)	AT&T Account Number: 989 R41 0229 718 4		X		NSO	8/23/2018	Monthly	50 MBPS	$752.64/mo 3/21	$9,031.68

T1 PRI Circuit - Mulholland	special T1 circuits - Primary Rate Interface carries voice and data between network and end user	Renewal approved during 4/2015 board meeting, included unlimited intralata calls for $80/month	-	-	-	- Tel-Net - - - - - -	5/30/2020	Monthly	12 mos	- - - $440/mo - - - - -	-
T1 PRI Circuit - for NSO site for BABH calls	special T1 circuits - Primary Rate Interface carries voice and data between network and end user	Renewal approved during 4/2015 board meeting, included unlimited intralata calls for $80/month	-	-	-	Tel-Net	5/30/2020	Monthly	12 mos	- - - $440.65 - - - -	-
PRI - Arenac Center	special T1 circuits - Primary Rate Interface carries voice and data between network and end user	TelNet Account Number: TN021779	-	*	-	TelNet	- - - - - - - -	Monthly	-	$405.15	-
PRI - Madison	special T1 circuits - Primary Rate Interface carries voice and data between network and end user	TelNet PRI - Account # TN021871 Order # TNN4589753	-	*	-	TelNet	- - -	Monthly	-	$421.70	-

		Circuit ID PPTHT1000041168									
Omnilert - Mass Notification System	Omnilert - mass notification system for alerting staff of emergent situations via email, SMS, and calling cell and desk phones	Licensed for 425 Users. 250 staff contacts and 2 contacts for each provider.	-	*	-	Omnilert	9/28/2021	9/28/2022	378 users	Platform Cost $1,800/yr User $4.20/yr (378 users)	$3,388
Ruckus Wireless - NSO	-	Support license renewals for controller and access point licenses; provides the latest patches and free warranty replacement if the device fails. This renewal is being done through Abadata at this time.	14	-	-	NSO/Ruckus	10/21/2022 6/3/2024	10/21/2023 6/3/2027	-	$170/month	-
Fortinet UTM Firewall Support includes FW hardware, FortiMgr support, and IOS subscriptions	-	Support for Fortinet UTM firewalls. Includes all branch firewalls and main FW at NSO network hub; support for Forti-Mgr and Forti-Analyzer servers; subscription for ongoing threat to keep security devices	-	*	-	NSO/Fortinet	11/1/2020	11/1/2025	-	Prepaid 5-year term.	$464/yr

		upgraded. Bought service with 5-year term when purchasing equipment.									
-	-	-	-	-	-	-	-	-	-	-	-
SSL Certificate - Wild Card	for multiple use *babha.org	-	-	-	-	Go-Daddy	- - 5/20/2022	5/20/2023	one multi-use cert	- $449.99 -	$449.99
-	-	-	-	-	-	-	-	-	-	-	-
Domain Registration Account - babha.org	web domain for access to network for BABHA	Some domains are through Go-Daddy; others through Network Solutions	-	-	X	-	-	10/9/2025	-	Prepaid 5-year term $105.85	$21.17
-	-	-	-	-	-	-	-	-	-	-	-
Adobe	Acrobat used to update PDF documents	BABH has 5? Adobe subscriptions – Acrobat (T Adler, J Louks,S. McRae, B. Beck; Medical Records Associate);	X	-	-	-	Acrobat - May 2013	n/a	Acrobat – IS Help Desk Specialist, T Adler, S. McRae, B. Beck, Medical Records Associate	Acrobat - $14.99/month/user	179.88 /user

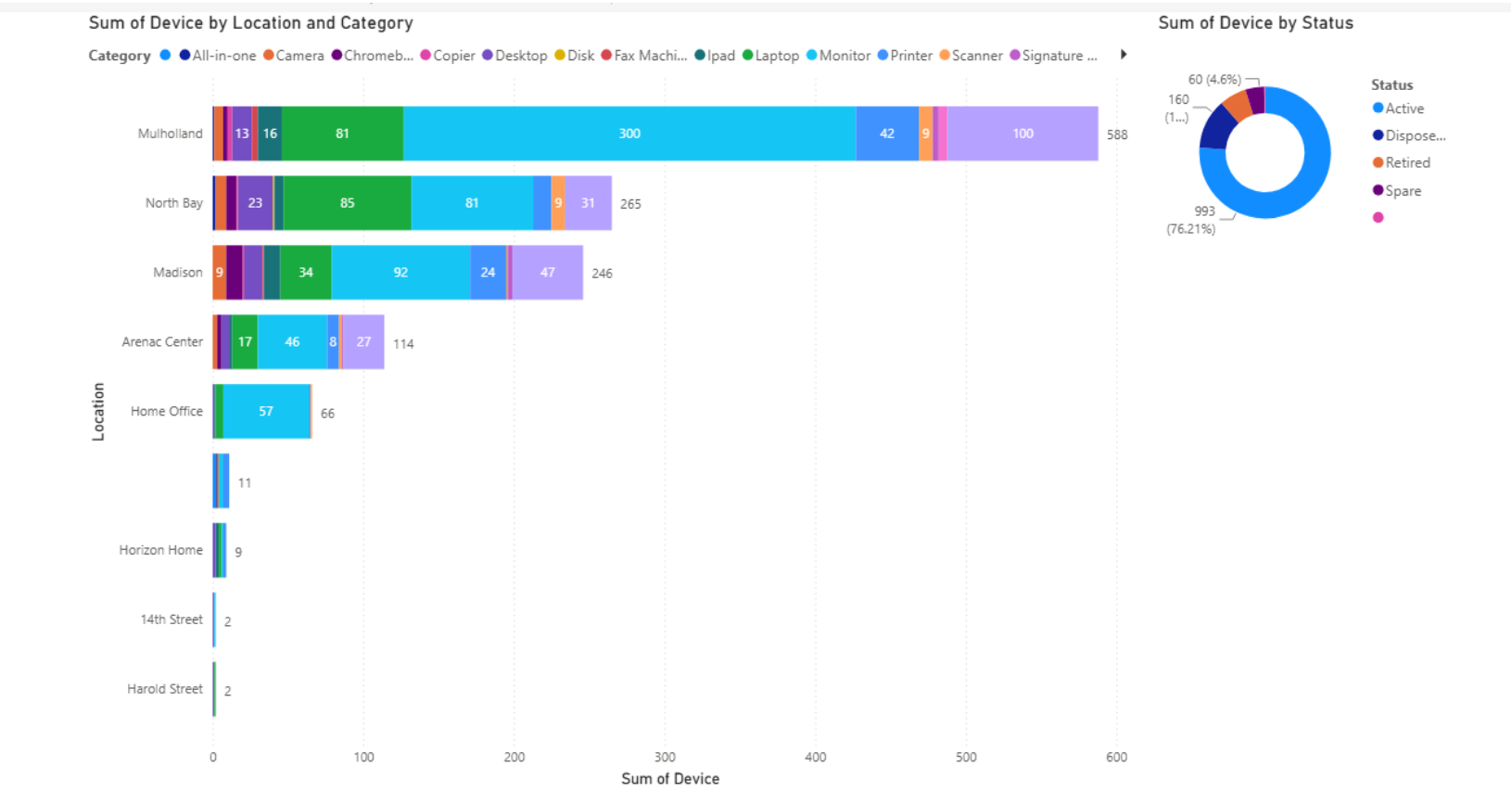
Fixed Asset Software (Sage)	Finance - asset management	handled by Finance directly	X	-	-	-	11/1/2020	11/1/2021	5 licenses	$3,211/yr	$3,211/yr
PCE Clinical Information Systems	EMR Implementation	-	-	-	-	-	9/20/2013	3/3/2014	-	$219,940	-
PCE Clinical Information Systems	ASP Services	-	-	-	-	-	3/1/2020	2/28/2023	-	$21,600/Month	-
PCE Clinical Information Systems	EPCS	E-prescribing (including controlled substances) for 10 prescribers	X	-	-	-	1/16/2014	evergreen	10 licenses	$1,500/month per prescriber	$18,000.00
CAFAS (Functional Assessment Systems)	web service with Multi-Health Systems	to permit PCE-Phoenix integration w/ CAFAS/ PECAFAS	-	-	-	-	3/12/2015	3/12/2016	implementation fee and annual fee	$1,999 implementation fee $499 annual fee	$1,999
SpeechExec Pro Transcribe	Dictation software for Madison Clinic	-	-	-	-	-	#1 01/2022 #2 08/19/22	#1 01/2024 #2 08/19/24	Two licenses	$254.15 per two-year subscription	$254.16
Jam Software - TreeSize Professional	program used to monitor/report file sizes, folders, folder permissions.	-	-	-	-	-	9/1/2022	8/31/2023	1 license – T.Adler	$27.98/year	$27.98
MSDN (Microsoft Developer Network)	software development tools used by Greg W and Greg L; Visual Studio is obtained	Licenses have been established for both Lisa Nagel and Greg Lietzow	X	-	-	Vendors	##########	##########	-	$799 (for GL renewal)	n/a

~~was through PC Connection; now CDW~~ - - - - - - -	~~through MSDN; (used for Gallery)~~					~~based on price~~			- ~~2 licenses – LNagel and GLietzow~~ - - - - - -		
~~Telerik DevCraft Support and Maintenance~~	~~software development tools (used for Gallery)~~	~~Reduced from 5 licenses to 2~~	~~X~~	~~X~~	-	-	~~2/27/2021~~	~~2/27/2022~~	~~2 licenses~~	~~$606.69 ea (inc 10% discount and govt discount)~~	~~$1,213.38~~

Commented [GL7]: @Lisa Nagel we did one license right..

IT Asset Management Dashboard

08/03/2026



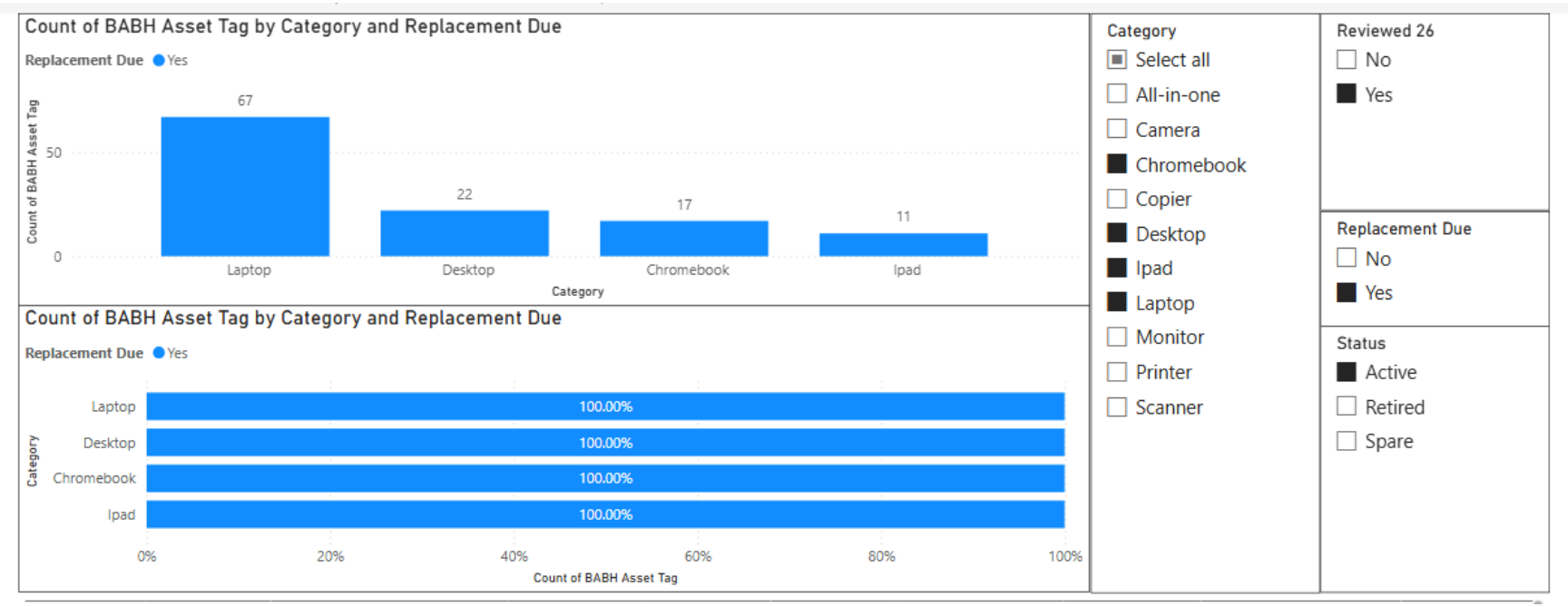
IT Asset Management Summary

The organization maintains an inventory of approximately 1,300 technology assets distributed across multiple service locations, with the majority located at the Mulholland, North Bay, and Madison offices. Inventory includes laptops, desktop

computers, monitors, printers, iPads, network devices, and other technology resources necessary to support operations and service delivery.

Asset management data indicates that more than three-quarters of all devices remain in active service, while a smaller number are designated as spare, retired, or pending disposal. Ongoing inventory management and lifecycle replacement efforts help ensure technology resources remain secure, functional, and available to support agency operations.

Key Takeaway: The agency continues to maintain a well-managed technology inventory with the majority of devices in active use. Regular monitoring of asset status and replacement cycles supports operational efficiency, cybersecurity, and business continuity.



Technology Asset Replacement Summary

Annual technology asset reviews identified 117 active devices that have reached or exceeded their planned replacement lifecycle, including 67 laptops, 22 desktop computers, 17 Chromebooks, and 11 iPads. Laptops represent the largest replacement need and reflect the agency's continued reliance on mobile technology to support operations and service delivery.

The replacement review process helps ensure aging equipment is identified and prioritized for future budgeting and procurement activities. Maintaining a structured device replacement strategy supports cybersecurity, system reliability, staff productivity, and business continuity by reducing the risk of hardware failures and unsupported technology. This has been incorporated into the BABHA Information Management Strategic Operating Plan.

Key Takeaway: Technology assets continue to be actively monitored through the agency's lifecycle management program, with replacement planning focused on maintaining secure, reliable, and efficient technology resources across the organization.

Replacement schedule from IMSOP

Device Type	Replacement Schedule
Desktop Computers	Replace devices every 4 years
Standard Laptop Computers	Replace devices every 4 years
Chromebooks	Replace devices every 4 years
iPads/Tablets	Replace devices every 3 years
10ZiG Thin Clients	Replace devices every 6 years
Desktop Printers	Replace devices every 6 years
Computer Monitors	Replace devices every 8 years

Replacement Cost

Device Type	Quantity	Unit Cost	Total Cost
Chromebooks (swap w/ surface)	17	$1,500	$25,500
Laptop	57	$1,500	$85,500
Desktop	17	$1,000	$25,500
iPad	3	$449	$1347
Total			$137,847