COLONIAL BEHAVIORAL HEALTH
BOARD MEETING

DATE: March 3, 2026

LOCATION: Colonial Behavioral Health, 473 McLaws Circle, Williamsburg, VA 23185

WELCOME AND CALL TO ORDER: 3:00pm

BOARD MEMBERS PRESENT:
Mr. John Collins – York County
Ms. Lynette Diaz – James City County
Mr. Sean Dunn – Williamsburg
Mr. Bruce Keener – York County
Ms. Kristen Nelson – York County
Mr. Gerald Patesel – Poquoson
Ms. Amber Richey – York County
Ms. April Thomas – York County
Ms. Donyale Wells – James City County
Mr. Roy Witham – James City County

BOARD MEMBERS ABSENT:
Mr. Ryan Ashe – James City County
Dr. Dawn Ide – City of Poquoson
Mr. Steven Miller – York County

CBH STAFF PRESENT:
David Coe, Marsha Obremski, Kristy Wallace, Kyra Cook, Patty Hartigan, and Denise Kirschbaum

GUESTS: None

PUBLIC COMMENT: None

CONSENT CALENDAR:
The consent calendar was presented for approval of the following meeting minutes:

- **February 3, 2026, Board of Directors Meeting**
- **February 17, 2026, Executive Committee Meeting**

The motion passed as follows:
Yes – 10
No – 0
Abstain – 0

DISCUSSION

Annual Board Planning Day

In the past, CBH has held an Annual Board Planning Day. Unfortunately, this training day was canceled in 2025. This training usually takes place in July/August although it could take place in another month. Sometimes, these planning days last a full day. A suggestion has been made to split the day in two: having dinner and a meeting and then breakfast and finishing the meeting the following day. Bruce Keener asked CBH Board members to check their calendars to see what dates will work/will not work. The following topics have been discussed during the Board Training Day: strategic planning, policies, future look, training topics, etc.

VACSB Board of Directors – Future Vacancies

The Virginia Association of Community Service Boards (VACSB) is made up of forty (40) CSB throughout the state. Virginia is divided into five (5) regions (CBH is a part of Region 5). The VACSB has a Board of Directors, usually comprised of two (2) members from each region. Recently, there was a vacancy for Region 5 although it was filled quickly. Any board member is welcome to attend the VACSB conferences – there are two conferences a year; one in January (training) and the second is in October (legislative). If a CBH Board member is interested in attending, please let David Coe know. Also, if a Board member would like to serve as a VACSB Board member, also let David know so he can put in a word ahead of time.

ACTION ITEMS:

A-1 Approval – Revisions to IS Policy 10 – Information Services *(Katie Leuci)*
A-2 Approval – Revisions to IS Policy 20 – General Technical Safeguards and Access Controls *(Katie Leuci)*
A-3 Approval – Revisions to IS Policy 21 – Security Updates and Security Training *(Katie Leuci)*
A-4 Approval – Revisions to IS Policy 22 – Workstation Use and Security *(Katie Leuci)*
A-5 Approval – Retirement of IS Policy 23 – IT Change Management *(Katie Leuci)*
A-6 Approval – Revisions to IS Policy 24 – Review of Information Systems Activity *(Katie Leuci)*
A-7 Approval – Revisions to IS Policy 25 – Response to Security Incidents *(Katie Leuci)*
A-8 Approval – Revisions to IS Policy 26 – Contingency Plans *(Katie Leuci)*
A-9 Approval – Revisions to IS Policy 27 – Risk Analysis and Risk Management *(Katie Leuci)*
A-10 Approval – Retirement of IS Policy 28 – Device and Asset Controls *(Katie Leuci)*
A-11 Approval – Revisions to IS Policy 29 – Facility Access Controls *(Katie Leuci)*
A-12 Approval – Revisions to IS Policy 30 – Malicious Software Protection *(Katie Leuci)*
A-13 Approval – Revisions to IS Policy 31 – Password Management and Log-In Monitoring *(Katie Leuci)*
A-14 Approval – Retirement of IS Policy 32 – Transmission Security Guidelines *(Katie Leuci)*

Bruce Keener and Katie Leuci presented the Protected Health Information set of policies (listed above) to the Board for approval. Changes to these policies have been made in consultation with and endorsed by Pat McDermott (legal counsel).
This set of policies were created in response to the security breach. The major update to all policies was transferring them to the template for.

Approval of A-1

IS Policy 10 – Information Services incorporates Policy 40 – Electronic Protected Health Information. Sean Dunn made a motion that the Board approve revisions to the Information Services policy as presented. John Collins seconded this motion. The motion passed as follows:
Yes – 10
No – 0
Abstain – 0

Approval of A-2 – A-14

Bruce Keener summarized the proposed changes to the remaining IS Policies which involve formatting to reflect the new policy template structure. Sean Dunn made a motion that the Board approve the revisions to the remaining IS Policies as presented. Amber Richey seconded the motion. The motion passed as follows:
Yes – 10
No – 0
Abstain – 0

REPORTS:

Fundraising Update (*Kyra Cook/Allison Brody*)

Kyra Cook introduced Allison Brody, Capital Campaign Fundraising position. Allison Brody comes to CBH with an extensive background in the non-profit, philanthropic, and mental health worlds. Allison explained the importance of testimonies – stories from our Board members. Allison was asked what are two low-cost initiatives that she will utilize during the campaign: 1. AI and 2. Coffee. Allison shared her "elevator speech" regarding Phase 2.

Facility Development Report *(Kyra Cook)*

Center for Support and Wellness (Phase 1)

The project remains on schedule. Budget update: certain costs remain within the overall project budget but exceed the original contract with Henderson: unsuitable soils – this was previously discussed with the Board. Partially collapsed stormwater system on the parcel across the street (future Phase 2 location). The decision on repair was delayed until Phase 2 vendor selection due to its location. Now that Phase 2 vendor has been selected, we've requested a price from Henderson. Our hope is to address the stormwater system as a Phase 1 change order, coordinated with the Phase 2 design. Amount of the change order is pending; we will update the Board once available.

Phase 2

Vendor Selection: The Henderson/Guernsey Tingle team has been selected following a competitive process. The decision was challenging given the quality of the proposals. SEVHS staff participated actively in interviews and discussions. Our owner's representatives provided

thoughtful questions and insights.

Next Steps

We are currently negotiating the contract, with a goal to bring it to the Board for action in April. By the Phase 1 ribbon cutting, we aim to have completed the following: site master plan for the entire parcel, exterior elevations, interior renderings, and block floor plan.

Funding update

Current contributions include $600K from the Williamsburg Health Foundation and $50K from the Clark Foundation. These funds will cover a significant portion of Phase 2; we ***may*** need to use year-end fund balance to fully bridge the gap, which will be included in the April Board recommendation. Initially, we anticipated more financial flexibility due to the funding secured by Delegate Wittman. The USDA funding process has proven to be challenging: the funds were congressionally directed, so the USDA should not have discretion over approval. The application was thorough and transparent; we expect eventual approval. However, due to staffing reductions and atypical funding requirements, resolution may take some time. We cannot wait for federal approval before proceeding but that could possibly impact our access to those funds.

Board Action in April

Staff will present recommendations, and if funding clarity is not fully achieved, staff may recommend moving forward with Phase 2 to maintain schedule. Kyra Cook is happy to answer any questions now or at the April Board meeting.

Recruitment/Hiring/Retention Report *(David Coe)*

For the period of January 15, 2026, through February 11, 2026, Colonial Behavioral Health (CBH) successfully completed 7 hires (all full-time positions), and the agency has one additional full-time offer in a pending status. Pending acceptance of position, the agency will be recruiting 25 positions which include 10 full-time positions, 2 part-time positions and 4 PRN/WAR positions. CBH experienced 5 resignations (all full-time positions) during the reporting period and 1 orientation no-show.

Allison Brody (Capital Campaign Fundraiser), Neil Morgan (Budget Advisor) and the Director of Finance positions were part of the hires for this period.

The minimum wage increase will put pressure on the lower paid salaries within CBH.

December 2025 Financial Report (*David Coe*)

The Financial Report as of January 31, 2026, was included in the Board meeting packet.

Executive Director's Report (*D. Coe*)

<u>Agency Issues</u>

The VACSB Annual Training Conference will be held May 6-8 in Richmond. If you are interested in attending, please contact Kristy Wallace to manage your registration.

<u>Community Issues</u>

Licensed Child & Adolescent Therapist Casandra Jones is presenting a workshop at the American Group Psychotherapy Association (AGPA) conference on March 5th. The workshop is entitled *"An Introduction to Tabletop Role Palay Games (TT-RPG) as a Group Therapy Modality"*. The workshop will utilize the game *Dungeons & Dragons*.

We are currently presenting CBH's work to each locality's governing bodies. We have presented

(or are scheduled to present) as follows:

February 9th	7:00pm	Poquoson City Council
February 12th	2:00pm	Williamsburg City Council
February 24th	1:00pm	JCC Board of Supervisors
March 3rd	6:00pm	York County Board of Supervisors

David plans to highlight York County's Finance Staff – the assistance they have provided to CBH is greatly appreciated. Susan Goodwin has been fantastic to work with, and she has been very involved.

Public Policy

It appears that the $10 million budget amendments submitted by Senator McDougle and Delegate Anderson were not included in the Senate or House committee budget reports. These were intended to support Phase 2 of our facility expansion project. There were too many competing priorities.

A summary of the State Budget actions taken to date in the 2026 Regular Session of the General Assembly will be shared as soon as details are available on the GA website (David plans to share with the Board at the April meeting).

We are rapidly approaching the April 1st deadline for Virginia's SAMHSA application for inclusion in the CCBHC Demonstration program. 2028: CBH → CCBHC.

QUESTIONS

Bruce Keener asked for clarification on future payouts for employees:
June 2026 (this FY) 2% Bonus
July 2027 (next FY) 2% Pay Raise

ADJOURNMENT:

A motion to adjourn the meeting was made by John Collins and seconded by April Thomas. The motion passed as follows:
Yes – 10
No – 0
Abstain – 0
The meeting was adjourned at 3:40pm.

NEXT MEETING:

Date: Tuesday, April 7, 2026
Location: 473 McLaws Circle, Williamsburg, VA 23185
Time: 3:00pm

Ryan Ashe, Board Chair

Amber Richey, Secretary

AGENDA
COLONIAL BEHAVIORAL HEALTH
BOARD OF DIRECTORS
MARCH 3, 2026
3:00 PM

- **WELCOME AND CALL TO ORDER**

- **ROLL CALL**

- **PUBLIC COMMENT**

- **CONSENT CALENDAR**
  - Approval of the following meeting minutes:
    - February 3, 2026, Board of Directors Meeting
    - February 17, 2026, Executive Committee Meeting

- **DISCUSSION**
  - Annual Board Planning Day
  - VACSB Board of Directors – future vacancies

- **ACTION ITEMS**
  - A-1 Approval – Revisions to IS Policy 10 – Information Services (*K. Leuci*)
  - A-2 Approval – Revisions to IS Policy 20 – General Technical Safeguards and Access Controls (*K. Leuci*)
  - A-3 Approval – Revisions to IS Policy 21 – Security Updates and Security Training (*K. Leuci*)
  - A-4 Approval – Revisions to IS Policy 22 – Workstation Use and Security (*K. Leuci*)
  - A-5 Approval – Revisions to IS Policy 23 – IT Change Management (*K. Leuci*)
  - A-6 Approval – Revisions to IS Policy 24 – Review of Information Systems Activity (*K. Leuci*)
  - A-7 Approval – Revisions to IS Policy 25 – Response to Security Incidents (*K. Leuci*)
  - A-8 Approval – Revisions to IS Policy 26 – Contingency Plans (*K. Leuci*)
  - A-9 Approval – Revisions to IS Policy 27 – Risk Analysis and Risk Management (*K. Leuci*)
  - A-10 Approval – Revisions to IS Policy 28 – Device and Asset Controls (*K. Leuci*)
  - A-11 Approval – Revisions to IS Policy 29 – Facility Access

Controls (*K. Leuci*)

- A-12 Approval – Revisions to IS Policy 30 – Malicious Software Protection (*K. Leuci*)
- A-13 Approval – Revisions to IS Policy 31 – Password Management and Log-In Monitoring (*K. Leuci*)
- A-14 Approval – Revisions to IS Policy 32 – Transmission Security Guidelines (*K. Leuci*)

- **REPORTS**
  - Fundraising Update (*A. Brody*)
  - Facility Development Report (*K. Cook*)
  - Recruitment/Hiring/Retention Report (*C. Thomas*)
  - January 2026 Financial Report (*D. Coe*)
  - Executive Director's Report (*D. Coe*)
    - 2026 General Assembly update

- **Adjournment**

Next Meeting:
Tuesday, April 7, 2026
473 McLaws Circle, Williamsburg
3:00 PM

COLONIAL BEHAVIORAL HEALTH
BOARD MEETING

DATE: February 3, 2026

LOCATION: Colonial Behavioral Health, 473 McLaws Circle, Williamsburg, VA 23185

WELCOME AND CALL TO ORDER: 3:00pm

BOARD MEMBERS PRESENT:
Mr. John Collins – York County
Ms. Lynette Diaz – James City County
Mr. Bruce Keener – York County
Mr. Steven Miller – York County
Ms. Amber Richey – York County
Ms. April Thomas – York County
Mr. Roy Witham – James City County

BOARD MEMBERS ABSENT:
Mr. Ryan Ashe – James City County
Mr. Sean Dunn – Williamsburg
Dr. Dawn Ide – City of Poquoson
Ms. Kristen Nelson – York County
Ms. Donyale Wells – James City County

CBH STAFF PRESENT:
David Coe, Marsha Obremski, Kristy Wallace, Kyra Cook, Linda Butler, Patty Hartigan, Chaenn Thomas and Denise Kirschbaum

GUESTS: Pat McDermott (Legal Counsel)

PUBLIC COMMENT: None

CONSENT CALENDAR:
The consent calendar was presented for approval of the following meeting minutes:

- **January 6, 2026, Board of Directors Meeting**
- **January 22, 2026, Executive Committee Meeting**

John Collins made a motion to accept the consent agenda as presented. Steven Miller seconded the motion. The motion passed as follows:
Yes – 7
No – 0
Abstain – 0

BOARD MEMBER JOB DESCRIPTION
The Board Member Job Description was a part of the Board Specific Policies that were reviewed and approved by the Board in December 2025. A copy of the Board Member Job Description was provided for each Board member present; Board members were asked to sign, date and return the job description. The signed job descriptions will be kept on file at CBH's Administration Office.

ACTION ITEMS:

A-1 Approval – Revisions to Policy 02 - Confidentiality *(Katie Leuci/Marsha Obremski)*

A-2 Approval – Revisions to Policy 27 – Health Information *(Katie Leuci/Marsha Obremski)*

A-3 Approval – Revisions to Policy 40 – Electronic Protected Health Information *(Katie Leuci/Marsha Obremski)*

A-4 Approval – Revisions to Policy 49 – Business Associate Agreement *(Katie Leuci/Marsha Obremski)*

A-5 Approval – Retirement of Policy 52 – Electronic Signature *(Katie Leuci/Marsha Obremski)*

Marsha Obremski presented the Protected Health Information set of policies (listed above) to the Board for approval. Changes to these policies have been made in consultation with and endorsed by Pat McDermott (legal counsel).
Amber Richey made a motion that the Board approve revisions to the Protected Health Information policies and the retirement of Policy 52 – Electronic Signature. John Collins seconded this motion. The motion passed as follows:
Yes – 7
No – 0
Abstain – 0

A-6 Approval – Financial Support for One-Time PSAP Database Updates (Marcus Alert) *(Kyra Cook)*
Approval of a $50,000 allocation of Marcus Alert funding to the Peninsula Regional Emergency Communications Center (PRECC), the Public Safety Answering Point (PSAP) for our region. This request is brough to the Board in accordance with agency policy, as expenditures of $50,000 or more require Board approval.
Steven Miller made a motion that the Board approve the $50,000 allocation of Marcus Alert funding to the Peninsula Regional Emergency Communications Center. John Collins seconded this motion. The motion passed as follows:
Yes – 7

No – 0
Abstain – 0

REPORTS:

Fundraising Report (*Kyra Cook*)

The Capital Campaign Fundraiser position has been filled by Allison Brody; her first day with CBH was Monday, February 2. Allison Brody brings with her a wealth of fundraising knowledge, specifically with local, non-profit organizations. Allison previously worked for Child Development Resources (CDR) where she took fundraising efforts to the next level.

Facility Development Report *(Kyra Cook)*

The construction of the CSW is still on schedule despite the recent winter weather. CBH plans to bring contracts for inside furniture to the Board in three months for review. The RFPs for Phase 2 are due tomorrow; we will act on these during the March Board meeting. A public hearing will take place during the Executive Committee meeting on February 17th. CBH is advertising the public hearing on our website, EVA and the Daily Press.

Recruitment/Hiring/Retention Report *(Chaenn Thomas)*

For the period of December 10, 2025, through January 15, 2026, Colonial Behavioral Health (CBH) has successfully completed ten new hires (8 full-time and 2 PRN/WAR). The agency is currently recruiting for 27 positions, which include 21 full-time, 2 part-time, and 4 PRN/WAR positions. CBH had three PRN/WAR resignations during the reporting period.

Since January 15, 2026, CBH has made three offers for employment; both the Fundraising and Budget Advisor positions have been filled. CBH has 4 new hires scheduled for our next onboarding. We are advertising the Finance Director position although we are utilizing a professional recruitment firm to assist with this process. David Coe expects to receive a batch of resumes tomorrow; David Coe and Susan Goodwin will screen these on Friday. This will be a "recruit to hire" position (contract).

December 2025 Financial Report (*David Coe*)

David Coe reviewed the Financial Report as of 12/31/2025. Our operating budget remains consistent with previous month; this is due to timing issues, vacancies and our collection of no-show fees improved this year. We are also planning for year-end expenditure, involving a 2% one-time payment to employees in June and health insurance costs.

The Budget Advisor position has been filled by Neil Morgan; his first day with CBH was Monday, February 2. Mr. Morgan will be on board with CBH until June 2026 – his main goal will focus on how we can improve our budget process. CBH is beginning the budget process early this year – we will have a budget to review in May and approve in June.

Executive Director's Report (*D. Coe*)

<u>Agency Issues</u>

David Coe shared the "large check" ($2M) that was presented to CBH by Congressman Rob Wittman to support Phase 2 of our building project.

York County has been providing support to CBH's finance department since the Finance Director position is currently vacant. This partnership is fantastic.

Community Issues

CBH is setting up times to meet with each of our localities to present CBH's work. Meetings with Poquoson and James City County will take place in February. CBH will meet with York County at the beginning of March. CBH will also meet with the City of Williamsburg although that meeting date has not yet been determined.

Public Policy

We are pleased to announce that Senator McDougle submitted a budget amendment for $10M to support Phase 2 of our building project. Delegate Anderson also submitted a budget amendment for the same amount and project. We are grateful for both. Senator McDougle is our "lead" in this effort.

It is difficult to project outcomes for CSBs and for those we serve in this General Assembly session – new General Assembly and a new Administration. A draft budget should be available at the end of this month, providing an insight into what's in and what's out.

The new DBHDS Commissioner came directly from Fairfax-Falls Church CSB and is friendly to the system of care. A new DMAS Director has not yet been appointed; an acting director is in place until the end of March.

David Coe asked Patty Hartigan to inform the Board about the SIM Grant that CBH received. The purpose of this grant is to map the resources and needs of our community. Community members are involved, working together as one for the betterment of the community we live in.

CLOSED SESSION:

Steven Miller made the following motion to move to a closed session: I motion that the CBH Board convene a closed meeting as permitted under the Code of Virginia for the following purposes: Discussion of an employment matter pertaining to a specific employee who has faced a disciplinary action for performance and the repercussions of the employees' conduct, pursuant to Section 2.2-3711(A)(1) of the code of Virginia's Freedom of Information Act; and Consultation with legal counsel employed or retain by a public body regarding specific legal matters requiring the provision of legal advice by such counsel, pursuant to Section 2.2-3711.A.8 of the Code of Virginia's Freedom of Information Act. Roy Witham seconded this motion.

Steven Miller made a motion to conclude the closed session. John Collins seconded the motion, which was unanimously approved. Board members were individually polled immediately coming out of the closed session to certify that only those matters covered in the motion for closed session were discussed.

ADJOURNMENT:

A motion to adjourn the meeting was made by John Collins and seconded by Amber Richey. The motion passed as follows:

Yes – 7

No – 0

Abstain – 0
The meeting was adjourned at 3:55pm.

NEXT MEETING:
Date: Tuesday, March 3, 2026
Location: 473 McLaws Circle, Williamsburg, VA 23185
Time: 3:00pm

_____ _____

Ryan Ashe, Board Chair **Amber Richey, Secretary**

COLONIAL BEHAVIORAL HEALTH

EXECUTIVE COMMITTEE MEETING
473 McLaws Circle, Williamsburg
February 17, 2026, at 3:00pm

Call to Order:
The Executive Committee Meeting was called to order at 3:00pm.

Committee Members Present:
Bruce Keener, Amber Richey, John Collins, Donyale Wells

Committee Members Absent:
Ryan Ashe

CBH Staff Present:
David Coe, Marsha Obremski, Kyra Cook, Katie Leuci, Kristy Wallace

Members of the Public:
N/A

PUBLIC HEARING
Colonial Behavioral Health (CBH) will hold a public hearing to receive comments from interested parties regarding Public Private Education Facilities and Infrastructure Act (PPEA) proposals received from Henderson Inc. and Sussex Development. The proposals are regarding the design and construction of an outpatient and administrative facility on Ironbound Rd., between Schmidt Rd. and Galt Ln.
The public hearing was closed at 3:05pm.

UPDATES/DISCUSSION ITEMS
Recruitment/Hiring/Turnover Update (*Chaenn Thomas*)
For the period of January 15, 2026, through February 11, 2026, Colonial Behavioral Health (CBH) successfully completed 7 hires (all full-time positions), and the agency has one additional full-time offer in a pending status. Pending acceptance of this position, the agency will be recruiting for 25 positions which include 19 full-time positions, two (2) part-time positions and four (4) PRN/WAR positions. CBH experienced five (5) resignations (all full-time positions) during this reporting period and one (1) orientation no-show.
We will see a dramatic increase in vacancies when we begin hiring for the CSW positions once funding is received although this could take up to six (6) months.

January 2026 Financial Report (*David Coe*)
David reviewed the Financial Report as of 1/31/2026. CBH is in good shape based on our operating margin although this is due to our number of vacancies and underspent dollars. CBH aims to have

3-6 months in reserve. Licensure requires three (3) months and DBHDS frowns upon anything more than three (3) months. Currently, federal and state money is combined – CBH will separate this out.

Finance Director Vacancy (*David Coe*)
Nancy Parsons (Director of Finance) retired from CBH on December 31, 2025, and this position is currently vacant. We are moving forward with the 2nd round of interviews with two (2) candidates provided to CBH through the headhunter services.

ANTICIPATED ACTION ITEMS – 3/3 BOARD MEETING

Information Services Group (*Katie Leuci*)
Katie Leuci presented and reviewed any updates to the following Information Services Policies:

- IS Policy 10 – Information Services
- IS Policy 20 – General Technical Safeguards and Access Controls
- IS Policy 21 – Security Updates and Security Training
- IS Policy 22 – Workstation Use and Security
- IS Policy 23 – IT Change Management
- IS Policy 24 – Review of Information System Activity
- IS Policy 25 – Response to Security Incidents
- IS Policy 26 – Contingency Plans
- IS Policy 27 – Risk Analysis and Risk Management
- IS Policy 28 – Device and Asset Controls
- IS Policy 29 – Facility Asset Controls
- IS Policy 30 – Malicious Software Protection
- IS Policy 31 – Password Management and Log-In Monitoring
- IS Policy 32 – Transmission Security Guidelines

Policy 10 had the most changes and will absorb Policy 40 – Electronic Protected Health Information. The above policies and accompanying revisions have been reviewed and endorsed by Pat McDermott (legal counsel).

OTHER ITEMS for 3/3 BOARD

Facilities Update *(Kyra Cook)*
Still on target for Fall 2026 opening. Henderson is wrapping up outside steel work.

Fundraising Update (*Allison Brody*)
Allison Brody will introduce herself to the Board of Directors.

General Assembly Updates (*David Coe*)
David Coe will provide an update on the General Assembly. The budget (House and Senate) should be available by the end of next week. The spreadsheet will not be included in the Board packet although David will present it during the Board meeting. A few items that

could affect CBH: minimum wage (issue with retention) and collective bargaining. Sick leave will not be an issue because it is already provided.

Executive Director's Report (*David Coe*)
This information will be included in the March Board Meeting packet.

DISCUSSION

Office Building Near Water Country (*Amber Richey*)
Amber Richey asked if CBH had moved into the office building near Water Country. Yes, we moved into the building in December. Our IT department is still working through some technical issues (scanning and printing) due to an internet issue (dead zone).

Items from the Committee

Finance Director: John Collins asked David if he thinks we will have a Finance Director by the March Board meeting. David's response was "not likely."
VACSB Board of Directors: David mentioned that it is nomination season for the VACSB Board of Directors. VACSB asked if there were any CSBs that have board members that would like to be on the VACSB board? CBH has never been a part of the VACSB Board of Directors. David can send an email to CBH Board of Directors. The Tidewater area has not been well represented. The time commitment would be 6 meetings, 3 of these would take place at the conferences with 1 in between.
Annual Board Planning Day: Bruce Keener asked if CBH was going to have the Annual Board Planning Day this year (we did not have one in 2025). A few items that could be discussed during a planning day would be strategic planning, FOYA, William & Mary Civic Committee, and Conflict Amongst Stakeholders. Ideas for increasing attendance could include Dinner meeting and breakfast/lunch meting the following day. We currently have 13 seated board members, 7 required for a quorum. Guest speaker: Jennifer Faison with the VACSB.
NEXT STEP: We need to determine the date of training soon.
Governor Glenn Youngkin: It was proposed that we invite Governor Glenn Youngkin back to the CSW at it's opening – provide a resolution?

Adjournment

John Collins made a motion to adjourn the meeting at 3:55pm. Amber Richey seconded this motion; all were in favor.

NEXT MEETING

Monday, March 16, 2026
2:00pm
473 McLaws Circle, Williamsburg, VA 23185

Action Item 1

Revision of IS Policy 10 – Information Services

Background:

CBH staff have reviewed the CBH Information Services Policy (Policy IS-10) and are pleased to recommend revisions to the Board of Directors for review.

A primary theme of the recommended changes is combining Policy 40 – Electronic Protected Health Information elements into IS-10 Information Services. IS-10 Information Services policy was originally reviewed and edited in 2025 by Liz Heddleston of Woods Rogers and the agency's lawyer, Pat McDermott.

This policy and accompanying revisions have been reviewed and approved by the agency's lawyer, Pat McDermott.

Summary of Changes:

Current Information Services Policy	Proposed Changes to Policy
Does not contain elements from Policy 40 – Electronic Protected Health Information.	Combine Policy 40 – Electronic Protected Health Information into IS-10 Electronic PHI section. Information about ePHI contained within Policy 40 aligns with IS Policy elements.
Sections for Distribution of Policies and Procedures, Submitting New or Revised Policies or Procedures, and Posting New or Revised Policies or Procedures referencing who posts to the CBH Intranet.	Move these elements to a Procedure.
There are no other changes from the 4/2025 approved policy.	

Motion from the CBH Executive Committee:

That the Board approve the revisions to Information Services policy as presented, including the incorporation of ePHI (Policy 40).

COLONIAL BEHAVIORAL HEALTH

COUNSEL REVIEW OF BOARD POLICY

Name of Policy: **Information Services**
Category: **Administration and Operations**
Policy No.: **IS-10**

Review Date: **February 16, 2026**

Name of Counsel: Patrick B. McDermott, Esq.

Comments of Counsel:

1. **Virginia Code Compliance: No violation**

2. **Federal Law Compliance: Please add the following section from the Code of Federal Regulations from which the policy's definition of "encryption is derived: 45 CFR 164.304**

3. **Grammar and Punctuation: Approved**

4. **Comments: This policy refers to three CBH officers. Please ensure that one or more persons are always appointed in writing to these positions as this will ensure the integrity of any future disciplinary action. The positions are:**

    1. **Director of Information Services**
    2. **Security Officer**
    3. **Development and Communications Manager**

Note: Policy 40 is now redundant and should be terminated.

Patrick B. McDermott, Esq.

Signature of Counsel

Policy and Procedures

Category: Administration and Operations

Title: Information Services

Policy Number: IS-10

Primary Areas Affected: All

Policy and Procedures

Category:	Administration and Operations
Title:	Information Services
Policy Number:	IS-10
Primary Areas Affected:	All

Policy Statement

Colonial Behavioral Health (CBH) operates information systems to facilitate automation of administrative processes and provide data to support management decisions. Systems for an electronic health record, clinical appointment scheduling, client and third-party billing, human resource management, and financial accounting as well as standard office automation products such as word processing, spreadsheets, scheduling, and electronic mail are supported on the CBH network. Access is available to and from remote sites and to the internet. The following section of policies and procedures will serve as a guide to operate and maintain this complex system, to also include all Information Services' policies that start with 'IS', Policy 2 Confidentiality, Policy 14 Personnel (disciplinary action and sanctions section), Policy 76 Telework, and Policy 81 Business Continuity – Telework.

CBH will maximize the use of automation, within resource limits, to enhance staff efficiency and productivity and to collect and exchange information to best serve individuals and families receiving services at CBH. Electronic information and automated processes are subject to the same policies, procedures, requirements, and restrictions as apply to other processes, media, or formats. CBH will implement procedures to properly secure and safeguard system hardware, software, and data from loss and/or corruption. Computer software, which is made available to the employee by the agency, is protected by U.S. Copyright Law and will not be copied without permission from the copyright owner.

Only CBH employees (including students, interns, volunteers, and consultants) may be authorized to use a CBH computer, a computer assigned by the Director of Information Services or designee, or a CBH issued mobile device when accessing ePHI. Visitors may be permitted to use a CBH computer only if preauthorized by the

Policy and Procedures

Category:	Administration and Operations
Title:	Information Services
Policy Number:	IS-10
Primary Areas Affected:	All

Director of Information Services or designee. The visitor will be required to use a local user account created and assigned by the Director of Information Services or designee.

HIPAA Employee Sanctions

Colonial Behavioral Health (CBH) will ensure the security of all ePHI through the diligent enforcement of CBH's policies and procedures. Any employee or workforce member who violates any of CBH's policies related to HIPAA, data security, or who takes any action which could compromise the security of ePHI, may be subject to disciplinary actions or sanctions in accordance with CBH Personnel Policies. **45 CFR § 164.308(a)(1)(ii)(C)**

HIPAA Security Rule Periodic Evaluation

The Security Officer, or designee, of Colonial Behavioral Health (CBH) shall conduct a periodic evaluation of the agency's policies and procedures to determine the extent to which they comply with the HIPAA Security Rule. The evaluation will include reviews of the technical and non-technical aspects of CBH's security program and is intended to assess whether CBH maintains appropriate security measures and policies to comply with the HIPAA Security Rule. The periodic evaluation should take place at least annually, or more frequently in response to environmental and operational changes that affect the security of CBH's ePHI. **45 CFR 164.308(a)(8)**

The Security Officer will designate employees who are responsible for determining when evaluation is necessary due to environmental or operational changes impacting ePHI. The results of such evaluation shall be documented by the Security Officer and retained by CBH for a period of at least six years from the date of the evaluation. The Security Officer shall be responsible for implementing steps necessary and reasonable under the circumstances to address any issues identified by such an evaluation.

Policy and Procedures

Category:	Administration and Operations
Title:	Information Services
Policy Number:	IS-10
Primary Areas Affected:	All

Assistive Technology

For individuals with special needs due to disability or impairment, the CBH program may provide, coordinate with community resources, or make referrals for assistive technology to include devices used to increase, maintain, or improve functional capabilities. The CBH program may also implement reasonable accommodation strategies which enable the individual to participate in services. Examples include: Braille, video or audio instruction, translated material, and augmented communication technology. At a minimum, individuals that utilize software involving audio assistance must utilize headphones to safeguard PHI.

Electronic Mail

CBH provides internal and external electronic mail (e-mail) as an effective communication and information-gathering tool. E-mail is to be used solely for business purposes. It may not be used to disseminate PHI unencrypted. All e-mail use is governed by applicable CBH policy and procedure.

Distributing abusive, offensive, pornographic, or other inappropriate material is prohibited as is dissemination of information not related to official business.

CBH provides a secure mail solution for confidential correspondence. Please see the IS-32 Transmission Security Guidelines Policy for more information regarding encryption and transmission of ePHI using email or messaging systems.

Policy and Procedures

Category:	Administration and Operations
Title:	Information Services
Policy Number:	IS-10
Primary Areas Affected:	All

Electronic PHI

Protected health information (PHI) is private and confidential, as stipulated in CBH Policy 2 – Confidentiality. Electronic PHI (ePHI) is subject to the same privacy and confidentiality restrictions as non-electronic PHI. Accordingly, each CBH employee is responsible for the security of electronic PHI. Each employee is responsible for compliance with this policy, as indicated by their signature on the Electronic Protected Health Information Employee Agreement. Electronic PHI may only be saved on a secure network drive, such as the user's Home Directory ("H"), assigned OneDrive, or a group folder within the "W" drive. Electronic PHI may not be saved to the internal memory or hard drive of a personal computer or mobile device unless administratively authorized by the agency's Director of Information Services with appropriate additional security measures, such as BitLocker.

Colonial Behavioral Health leadership provides specified employees the authority to document and electronically sign documents in the agency's legal health record. Under no circumstance shall the employee use their password to sign electronic documents for services delivered by any other provider. The employee's signature password shall be used to authenticate and attest documents in the electronic health record for whom the respective employee provides services or for entries generated by the employee as delineated in policy. By this policy, each employee certifies that they will not disclose their password to any other person or permit another person to use their password for the purposes of documenting in the health record. By this policy, each employee is informed that Colonial Behavioral Health has the right to terminate employment of any employee determined to have misused or permitted another individual to sign electronically any legal health documents on their behalf.

Policy and Procedures

Category:	Administration and Operations
Title:	Information Services
Policy Number:	IS-10
Primary Areas Affected:	All

Distribution of Policies and Procedures

The official means of distributing policies and procedures will be via posting on the CBH Intranet. All employees and workforce members are responsible for reviewing information on the Intranet as frequently as necessary to ensure their knowledge is current. Any employee or workforce member unable to access a workstation for this purpose is responsible for consulting their supervisor to arrange access.

Intranet Administrator

The Development and Communications Manager is the administrator for the Intranet. They, or their designee, will maintain electronically signed documents on the Intranet, word processing source documents in a separate directory, and previous versions of documents in an archive directory. The Development and Communications Manager or designee will manage the process for revision, review, and final posting of information to the Intranet. Documents can be submitted via e-mail through supervisory channels to the appropriate program director or designee. Upon approval, the program director or designee will forward the document via ticket system or e-mail indicating approval to the Development and Communications Manager.

The Development and Communications Manager or designee has the latitude to delete documents from the Intranet. Documents may be deleted from the Intranet by the Development and Communications Manager or designee with authorization from the program director or the program director's designee who was previously responsible for the posting of the document.

Source of Authorization

Board of Directors

Policy and Procedures

Category:	Administration and Operations
Title:	Information Services
Policy Number:	IS-10
Primary Areas Affected:	All

Legal/Regulatory References

45 CFR 164.304

45 CFR § 164.308(a)(1)(ii)(C)

45 CFR 164.308(a)(8)

45 CFR 160.103

12VAC-115-80

Definitions

1. **Encryption** is defined as: "the use of an algorithmic process to transfer data into a form in which there is a low probability of assigning meaning without use of a confidential process or key and such confidential process or key that might enable decryption has not been breached."
2. PHI is defined in 45 CFR 160.103. PHI can be in the form of text, picture, or video.

Policy and Procedures

Category:	Administration and Operations
Title:	Information Services
Policy Number:	IS-10
Primary Areas Affected:	All

Diary of Changes

Date of Origin

10/1/2000

Dates of Review

6/15/2023	4/30/2025	3/3/2026

Dates of Revision

10/24/2025	4/30/2025	3/3/2026

Approved By

_____	_____
Signature	Effective Date
_____	CBH Board Chair
Printed Name	Title

Action Item 2

Revision of Policy IS-20 – General Technical Safeguards and Access Controls

Background:

CBH staff have reviewed the CBH General Technical Safeguards and Access Controls Policy (Policy IS-20) and are pleased to recommend revisions to the Board of Directors for review.

IS-20 General Technical Safeguards and Access Controls policy was originally reviewed in 2025 by Liz Heddleston of Woods Rogers and the agency's lawyer, Pat McDermott.

This policy and accompanying revisions have been reviewed and approved by the agency's lawyer, Pat McDermott.

Summary of Changes:

Current General Technical Safeguards and Access Controls Policy	Proposed Changes to Policy
Old policy format	Formatted to reflect new policy template structure.
There are no other changes from the 4/2025 approved policy.	

Motion from the CBH Executive Committee:

That the Board approve the revisions to General Technical Safeguards and Access Controls policy as presented.

COLONIAL BEHAVIORAL HEALTH

COUNSEL REVIEW OF BOARD POLICY

Name of Policy: **General Technical Safeguards and Access Controls**
Category: **Administration and Operations**
Policy No.: **IS-20**

Review Date: **February 16, 2026**

Name of Counsel: Patrick B. McDermott, Esq.

Comments of Counsel:

1. **Virginia Code Compliance:** **No violation**
2. **Federal Law Compliance** **45 CFR 164.312(a)-(e)**
3. **Grammar and Punctuation:** **Acceptable**
4. **Comments:** **No Comments**
5. **Note:** **The policy that I reviewed had editorial comments in the margin. Should be finalized before board vote.**

Patrick B. McDermott, Esq.

Signature of Counsel

Policy and Procedures

Category: Administration and Operation

Title: General Technical Safeguards and Access Controls

Policy Number: IS-20

Primary Areas Affected: All

Policy and Procedures

Category:	Administration and Operation
Title:	General Technical Safeguards and Access Controls
Policy Number:	IS-20
Primary Areas Affected:	All

Policy Statement

Colonial Behavioral Health (CBH) will implement and maintain technical safeguards which ensure the confidentiality, integrity, and availability of all ePHI that CBH creates, receives, maintains, or transmits. Technical safeguards include technology and processes that protect ePHI and control access to it. These technical safeguards apply to the agency's on-premises, cloud, and hybrid environments.

Source of Authorization

Board of Directors

Legal/Regulatory References

HIPAA Security Rule, 45 CFR § 164.312(a)-(e)

Definitions

N/A

Procedures

The following is a summary of the technical safeguards and access controls that CBH uses to safeguard ePHI:

1. A unique name and/or number is used to identify and track the user identity of employees within CBH's electronic systems. Generic or shared account used to access ePHI is extremely limited and must be approved by the Security Officer. If a generic or shared account must be used due to a system limitation,

Policy and Procedures

Category: Administration and Operation

Title: General Technical Safeguards and Access Controls

Policy Number: IS-20

Primary Areas Affected: All

the Security Officer will be notified and the internal IS procedure for generic and/or shared account will be followed.

2. An Electronic Protected Health Information Agreement must be completed, signed and stored in an employee's personnel record.
3. An employee's supervisor must complete a System Access Request (SAR) form specifying which applications to which the employee may have access and type of access within those applications. A login and password will not be set up without a SAR. The access level granted to each employee or workforce member should be based on their job duties and workplace requirements. CBH should grant the minimum access necessary based on the employee or workforce members' formal role within the agency (i.e., "need to know"). Access levels will be reviewed and modified as needed on a periodic basis.
4. An employee shall ensure that the CBH device being used is properly secured against unauthorized use when unattended.
5. CBH shall implement procedures, including passwords and/or other verification methods, to authenticate any user seeking access to ePHI.
    a. All passwords must comply with CBH's password strength requirements.
    b. All passwords must be changed within the timeframe designated and required by the CBH IT Department.
    c. Passwords shall not be shared by employees or workforce members for any reason.
    d. Systems and applications shall not be configured to save passwords. If prompted, employees and workforce members shall not save their passwords when accessing the Electronic Health Record

Policy and Procedures

Category: Administration and Operation

Title: General Technical Safeguards and Access Controls

Policy Number: IS-20

Primary Areas Affected: All

(EHR), electronic systems/databases/applications used by CBH, or webpage portals that contain ePHI.

e. CBH shall review, as appropriate, workstation, OS and application access logs, as well as failed or successful changes to account permissions.

f. Each employee will be held responsible for all transactions performed using their login and password (including health record entries).

g. All of the above practices shall apply to vendors and third parties who have access to CBH's network and ePHI, as applicable.

6. CBH shall implement procedures and/or safeguards to verify that a person or entity seeking access to ePHI is the one claimed.

7. CBH shall implement multifactor authentication where possible and reasonably practical. This shall include requiring MFA for access to any virtual private network (VPN) used by CBH. MFA via the Microsoft Authenticator application is CBH's primary method of MFA.

8. CBH shall implement procedures to ensure that authorized users are able to access ePHI during an emergency. Emergency access procedures should not rely on the availability of a single individual.

9. CBH shall implement electronic procedures that terminate any electronic session at any agency computer, workstation or other access point after a reasonable predetermined time of inactivity. See the HIPAA Workstation Use and Security policy for additional information.

Policy and Procedures

Category: Administration and Operation

Title: General Technical Safeguards and Access Controls

Policy Number: IS-20

Primary Areas Affected: All

10. Logins and/or passwords for terminated employees, vendors, and third parties will be removed by the Information Services staff upon notification of termination of employment. CBH supervisors are responsible for notifying the Information Services staff of employee terminations via the SAR procedure.
11. CBH shall encrypt ePHI in transmission and at rest. Unencrypted ePHI will not be stored on portable electronic devices, including laptops. In situations where encryption is problematic or infeasible, an alternative safeguard must be implemented as appropriate, in consultation with the Security Officer and CBH's IT administrator. In these situations, the Security Officer will document the reasons for any lack of encryption and the alternative safeguards employed.
12. CBH shall implement hardware, software and/or procedural mechanisms that record and examine activity in the agency's information systems that contain or use ePHI.
13. CBH shall implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.
14. CBH shall back up necessary systems and data. CBH shall test the restoration process annually.
15. System and data access and use are governed by applicable CBH policy and procedure, including Confidentiality policy, Health Information policy, and the Electronic Protected Health Information Agreement. It is each employee's responsibility to learn and follow these requirements.
16. CBH's Director of Information Services or designee is responsible for approving use of outside software. No software acquired outside of CBH may be loaded onto CBH computers except by Information Services staff. Use of the software will be subject to the terms and license agreement associated with the product.

Policy and Procedures

Category:	Administration and Operation
Title:	General Technical Safeguards and Access Controls
Policy Number:	IS-20
Primary Areas Affected:	All

Diary of Changes

Date of Origin

2/6/2025

Dates of Review

3/3/2026

Dates of Revision

3/3/2026

Approved By

_____	_____
Signature	Effective Date
_____	CBH Board Chair
Printed Name	Title

Action Item 3

Revision of Policy IS-21 – Security Updates and Security Training

Background:

CBH staff have reviewed the CBH Security Updates and Security Training Policy (Policy IS-21) and are pleased to recommend revisions to the Board of Directors for review.

IS-21 Security Updates and Security Training policy was originally reviewed in 2025 by Liz Heddleston of Woods Rogers and the agency's lawyer, Pat McDermott.

This policy and accompanying revisions have been reviewed and approved by the agency's lawyer, Pat McDermott.

Summary of Changes:

Current Security Updates and Security Training Policy	Proposed Changes to Policy
Old policy format	Formatted to reflect new policy template structure.
There are no other changes from the 4/2025 approved policy.	

Motion from the CBH Executive Committee:

That the Board approve the revisions to Security Updates and Security Training policy as presented.

COLONIAL BEHAVIORAL HEALTH

COUNSEL REVIEW OF BOARD POLICY

Name of Policy: **Security Updates and Security Training**
Category: **Administration and Operations**
Policy No.: **IS-21**

Review Date: **February 16, 2026**

Name of Counsel: Patrick B. McDermott, Esq.

Comments of Counsel:

1. **Virginia Code Compliance:** **No violation**

2. **Federal Law Compliance** **42 CFR 164.308(a)(5)**
   42 CFR 164.308(a)(5)(I)
   42 CFR 164.308(a)(5)(2)(a)

3. **Grammar and Punctuation:** **Acceptable**

4. **Comments:** **Reference to CARF; Service Delivery Using Information and Communication Technology 2.13.**

Patrick B. McDermott, Esq.

Signature of Counsel

Policy and Procedures

Category: Administration and Operation

Title: Security Updates and Security Training

Policy Number: IS-21

Primary Areas Affected: All

Policy and Procedures

Category:	Administration and Operation
Title:	Security Updates and Security Training
Policy Number:	IS-21
Primary Areas Affected:	All

Policy Statement

Colonial Behavioral Health (CBH) will periodically provide training and "Security Updates" to all agency employees and workforce members to promote the security of CBH's ePHI and to reduce security risks. CBH shall take reasonable steps to ensure staff, including those who work remotely, are informed of information security risks on an ongoing basis and know how to follow the agency's security policies and procedures. CBH's Security Officer, or designee, shall be responsible for ensuring that all staff receive security awareness training at hire and periodically thereafter.

Source of Authorization

Board of Directors

Legal/Regulatory References

CARF; Service Delivery Using Information and Communication Technology 2.13, HIPAA Security Rule; 42 CFR 164.308(a)(5), 42 CFR 164.308(a)(5)(i), 42 CFR 164.308(a)(5)(ii)(A)

Definitions

N/A

Procedures

All employees and workforce members of CBH shall receive HIPAA security training within 10 days of hire, annually and periodically thereafter. This training should include information concerning how employees are

Policy and Procedures

Category: Administration and Operation

Title: Security Updates and Security Training

Policy Number: IS-21

Primary Areas Affected: All

expected to comply with the HIPAA Security Rule and guidance on how to protect the confidentiality and security of CBH's ePHI. The training will also cover CBH's procedures for guarding against, detecting and reporting suspected security incidents, including information concerning the importance of protecting against malicious software, social engineering, and other security threats. CBH may use an outside vendor to conduct training, however CBH's Security Officer must approve the content of such training to ensure it is adequate and meets HIPAA's requirements.

CBH shall develop periodic "Security Updates" for distribution to employees and workforce members regarding any material changes in the agency's Security Policies, procedures or systems and to generally maintain workforce knowledge and awareness of HIPAA Security Rule compliance. Security updates will cover key cybersecurity topics, such as encryption, multi-factor authentication, ransomware, social engineering, phishing, and emerging threats. CBH may use a variety of training tools to educate its workforce on security issues impacting PHI, including computer-based training, classroom training, newsletters, posters, email alerts and team discussions.

All security awareness training and "Security Updates" shall be tracked and documented in writing by CBH. Training records will be retained for at least six (6) years after completion of the training. These records will include dates and types of training, training materials, and evidence of workforce participation.

Policy and Procedures

Category:	Administration and Operation
Title:	Security Updates and Security Training
Policy Number:	IS-21
Primary Areas Affected:	All

Diary of Changes

Date of Origin

2/6/2025

Dates of Review

3/3/2026

Dates of Revision

3/3/2026

Approved By

_____	_____
Signature	Effective Date
_____	CBH Board Chair
Printed Name	Title

Action Item 4

Revision of Policy 22 – Workstation Use and Security

Background:

CBH staff have reviewed the CBH Workstation Use and Security Policy (Policy IS-22) and are pleased to recommend revisions to the Board of Directors for review.

IS-22 Workstation Use and Security policy was originally reviewed in 2025 by Liz Heddleston of Woods Rogers and the agency's lawyer, Pat McDermott.

This policy and accompanying revisions have been reviewed and approved by the agency's lawyer, Pat McDermott.

Summary of Changes:

Current Workstation Use and Security Policy	Proposed Changes to Policy
Old policy format	Formatted to reflect new policy template structure.
There are no other changes from the 4/2025 approved policy.	

Motion from the CBH Executive Committee:

That the Board approve the revisions to Workstation Use and Security policy as presented.

COLONIAL BEHAVIORAL HEALTH

COUNSEL REVIEW OF BOARD POLICY

Name of Policy: **Workstation Use and Security**
Category: **Administration and Operations**
Policy No.: **IS-22**

Review Date: **February 16, 2026**

Name of Counsel: Patrick B. McDermott, Esq.

Comments of Counsel:

1. **Virginia Code Compliance:** **No violation**
2. **Federal Law Compliance** **HIPAA Security Rule, 45 CFR 164.310(b)-(c)**
3. **Grammar and Punctuation:** **Acceptable**
4. **Comments:**
   a. **Insert "Administration and Operation" as Category.**
   b. **Probably delete link at bottom of page 4 of 5.**

Patrick B. McDermott, Esq.

Signature of Counsel

Policy and Procedures

Category:

Title: Workstation Use and Security

Policy Number: IS-22

Primary Areas Affected: All

Policy and Procedures

Category:

Title: Workstation Use and Security

Policy Number: IS-22

Primary Areas Affected: All

Policy Statement

Colonial Behavioral Health (CBH) will take reasonable steps to prevent unauthorized access to workstations that can access ePHI by implementing physical safeguards. For the purposes of this policy, a workstation is an electronic computing device, such as a laptop, desktop computer, or any other device that performs similar functions, as well as electronic media stored in the immediate environment of the device. The physical safeguards will be designed to prevent unauthorized access to ePHI while maintaining appropriate access for authorized workforce members.

Source of Authorization

Board of Directors

Legal/Regulatory References

HIPAA Security Rule, 45 CFR § 164.310(b)-(c)

Definitions

N/A

Policy and Procedures

Category:

Title: Workstation Use and Security

Policy Number: IS-22

Primary Areas Affected: All

Procedures

For the purposes of this policy, a workstation is an electronic computing device, such as a laptop, desktop computer, tablet, smart phone, or any other device that performs similar functions[i]. The definition of workstation also includes any electronic media stored in the immediate environment of the device. This policy applies to workstations located at CBH facilities as well as off-site workstations, such as those in a home office or another off-site location.

The following policies and procedures shall apply to all employees and workforce members that use any CBH workstation which permits access to ePHI:

1. When workstations are in private offices, the office must be locked when unoccupied for any extended period.
2. Care must be taken to restrict visual access to data/ePHI displayed on the workstation by positioning screens appropriately.
3. Workstations in private offices must be configured to either perform a locking screen-blank or automatically log off after a period of inactivity, not to exceed 30 minutes.
4. Any workstation used to access ePHI in a shared space must be configured with locking screen blanking, automatic log-out and screen positioning to minimize inappropriate viewing of data.
5. Workstations in shared space must be configured to either screen-blank or automatically log-off after some period of inactivity, not to exceed 15 minutes.
6. Employees and workforce members are required to log off applications containing ePHI or sensitive business information before leaving their workstations.

Policy and Procedures

Category:

Title: Workstation Use and Security

Policy Number: IS-22

Primary Areas Affected: All

7. In email, employees should not open attachments or click on links unless expecting them or first verify the legitimacy of the attachment or link with the sender. If an employee is in doubt about the legitimacy of an email message, or if an employee encounters suspicious behavior on their computer, employees must immediately notify the IT department before proceeding.
8. The internet is to be used solely for CBH business purposes. It may not be used to disseminate protected health information outside of CBH, except through a secure transmission approved by the Director of Information Services. All internet use is governed by applicable CBH policy and procedure.
9. Accessing abusive, offensive, pornographic, or other inappropriate material is prohibited.
10. Employees should browse the internet responsibility and not engage in social media, personal shopping or click on advertisements. Designated positions within the agency may use social media to carry out agency business with the Security Officer's approval.
11. Employees must not disable security settings on a workstation or stop or postpone scheduled updates, scans or reboots.
12. Employees must adhere to computer orientation training conducted by the CBH Information Technology department during the initial computer training provided by CBH. Topics discussed include, but are not limited to: appropriate use of CBH equipment, cord safety, how to properly clean touch screen, food and drink safety, etc.

Policy and Procedures

Category:

Title: Workstation Use and Security

Policy Number: IS-22

Primary Areas Affected: All

Diary of Changes

Date of Origin

2/6/2025

Dates of Review

3/3/2026

Dates of Revision

3/3/2026

Approved By

_____ _____

Signature Effective Date

_____ CBH Board Chair

Printed Name Title

Action Item 5

Revision of Policy IS-23 – IT Change Management

Background:

CBH staff have reviewed the CBH IT Change Management Policy (Policy IS-23) and are pleased to recommend revisions to the Board of Directors for review.

IS-23 IT Change Management policy was originally reviewed in 2025 by Liz Heddleston of Woods Rogers and the agency's lawyer, Pat McDermott.

This policy and accompanying revisions have been reviewed and approved by the agency's lawyer, Pat McDermott.

Summary of Changes:

Current IT Change Management Policy	Proposed Changes to Policy
Old policy format	Formatted to reflect new policy template structure.
There are no other changes from the 4/2025 approved policy.	

Motion from the CBH Executive Committee:

That the Board approve the revisions to IT Change Management policy as presented.

COLONIAL BEHAVIORAL HEALTH

COUNSEL REVIEW OF BOARD POLICY

Name of Policy: **IT Change Management**
Category: **Administration and Operations**
Policy No.: **IS-23**

Review Date: **February 16, 2026**

Name of Counsel: Patrick B. McDermott, Esq.

Comments of Counsel:

1. **Virginia Code Compliance:** **N/A**
2. **Federal Law Compliance** **N/A**
3. **Grammar and Punctuation:** **Acceptable**
4. **Comments:** **None**

Patrick B. McDermott, Esq.

Signature of Counsel

Policy and Procedures

Category: Administration and Operation

Title: IT Change Management

Policy Number: IS-23

Primary Areas Affected: All

Policy and Procedures

Category:	Administration and Operation
Title:	IT Change Management
Policy Number:	IS-23
Primary Areas Affected:	All

Policy Statement

Colonial Behavioral Health (CBH) shall work with its internal and external Information Technology (IT) team(s) to ensure that all material changes to the agency's information systems and technology are reviewed and approved prior to implementation. During and following implementation of changes, CBH shall ensure that the confidentiality, integrity, and availability of systems and data, including ePHI, are maintained. CBH shall retain documentation related to changes covered by this policy.

This Policy applies only to changes within the control of CBH. The types of changes that fall under this policy include but are not limited to:

- Changes to configuration of a SaaS application
- Deployment or removal of a SaaS application
- Implementation of updates, including security patches, or other changes to operating systems and applications on CBH devices
- Hardware changes to CBH devices
- Deployment or removal of IT devices

Source of Authorization

Board of Directors

Legal/Regulatory References

N/A

Policy and Procedures

Category:	Administration and Operation
Title:	IT Change Management
Policy Number:	IS-23
Primary Areas Affected:	All

Definitions

N/A

Procedures

1. Changes are approved by CBH's Security Officer or their designee.
2. Documentation of the approval must include clear identification of the change to be made as well as the timing of the change. An email from CBH's Security Officer to the IT team would be appropriate documentation.
3. Changes must be approved prior to deployment, but in an emergency or other unusual situation documentation may be finalized after deployment. For example, the Security Officer may approve the change by phone or chat and follow up with an email.
4. Changes are tested as appropriate.
5. Changes may be rolled back if needed. That is, the IT team must be able to return the systems to their pre-change settings.
6. Patches, especially security patches, are applied in a timely manner, usually within a week.
7. Post-deployment confirmation is documented. The Security Officer or designee will confirm that the expected results of the change have been achieved, and that no unexpected results have been detected.

Policy and Procedures

Category:	Administration and Operation
Title:	IT Change Management
Policy Number:	IS-23
Primary Areas Affected:	All

Diary of Changes

Date of Origin

2/6/2025

Dates of Review

3/3/2026

Dates of Revision

3/3/2026

Approved By

_____	_____
Signature	Effective Date
_____	CBH Board Chair
Printed Name	Title

Action Item 6

Revision of Policy IS-24 – Review of Information System Activity

Background:

CBH staff have reviewed the CBH Review of Information System Activity Policy (Policy IS-24) and are pleased to recommend revisions to the Board of Directors for review.

IS-24 Information System Activity policy was originally reviewed in 2025 by Liz Heddleston of Woods Rogers and the agency's lawyer, Pat McDermott.

This policy and accompanying revisions have been reviewed and approved by the agency's lawyer, Pat McDermott.

Summary of Changes:

Current Information System Activity Policy	Proposed Changes to Policy
Old policy format	Formatted to reflect new policy template structure.
There are no other changes from the 4/2025 approved policy.	

Motion from the CBH Executive Committee:

That the Board approve the revisions to Information System Activity policy as presented.

COLONIAL BEHAVIORAL HEALTH

COUNSEL REVIEW OF BOARD POLICY

Name of Policy: **Review of Information System Activity**
Category: **Administration and Operations**
Policy No.: **IS-24**

Review Date: **February 16, 2026**

Name of Counsel: Patrick B. McDermott, Esq.

Comments of Counsel:

1. **Virginia Code Compliance:** **N/A**

2. **Federal Law Compliance** **HIPAA Security Rule:**
   45 CFR 164.308 (a)(1)(ii)(D)

3. **Grammar and Punctuation:** **Acceptable**

4. **Comments:** **None**

Patrick B. McDermott, Esq.

Signature of Counsel

Policy and Procedures

Category: Administration and Operations

Title: Review of Information System Activity

Policy Number: IS-24

Primary Areas Affected: All

Policy and Procedures

Category:	Administration and Operations
Title:	Review of Information System Activity
Policy Number:	IS-24
Primary Areas Affected:	All

Policy Statement

Colonial Behavioral Health (CBH) will use security settings and other hardware, software and/or procedural mechanisms to record and examine activities on the agency's electronic information systems, including components of those systems (such as workstations). CBH shall assure that records of information system activity are regularly reviewed by outside vendors and in-house Information Technology (IT) professionals. The review may include the review of audit logs, event logs, firewall logs, system logs, data backup logs, access reports, anti-malware logs, and security incident tracking reports.

Source of Authorization

Board of Directors

Legal/Regulatory References

HIPAA Security Rule, 45 CFR § 164.308(a)(1)(ii)(D)

Definitions

N/A

Procedures

The purpose of this review is to ensure that CBH's implemented security controls are effective and that ePHI has not been potentially compromised. CBH will develop timeframes for reviewing different types of logs and activity that are reasonable and appropriate for the type of log or information that is being reviewed. Results of

Policy and Procedures

Category: Administration and Operations

Title: Review of Information System Activity

Policy Number: IS-24

Primary Areas Affected: All

CBH's information system review will be documented, including the identification of issues that may prompt further investigation. CBH will coordinate with external vendors and the CBH IT Department to conduct these activities. The CBH IT Department will immediately notify CBH's HIPAA Security Officer and senior leadership of any concerning events or activity detected through these reviews that may involve ePHI. CBH will ensure that its external IT and security vendors promptly escalate concerning events or system activity to the HIPPA Security Officer for further review and investigation. CBH will respond to suspicious activity in accordance with IS Policy 25 – Response to Security Incidents and/or other application policies and procedures.

Policy and Procedures

Category:	Administration and Operations
Title:	Review of Information System Activity
Policy Number:	IS-24
Primary Areas Affected:	All

Diary of Changes

Date of Origin

2/6/2025

Dates of Review

3/3/2026

Dates of Revision

3/3/2026

Approved By

_____	_____
Signature	Effective Date
_____	CBH Board Chair
Printed Name	Title

Action Item 7

Revision of Policy IS-25 – Response to Security Incidents

Background:

CBH staff have reviewed the CBH Response to Security Incidents Policy (Policy IS-25) and are pleased to recommend revisions to the Board of Directors for review.

IS-25 Response to Security Incidents policy was originally reviewed in 2025 by Liz Heddleston of Woods Rogers and the agency's lawyer, Pat McDermott.

This policy and accompanying revisions have been reviewed and approved by the agency's lawyer, Pat McDermott.

Summary of Changes:

Current Response to Security Incidents Policy	Proposed Changes to Policy
Old policy format	Formatted to reflect new policy template structure.
There are no other changes from the 4/2025 approved policy.	

Motion from the CBH Executive Committee:

That the Board approve the revisions to Response to Security Incidents policy as presented.

COLONIAL BEHAVIORAL HEALTH

COUNSEL REVIEW OF BOARD POLICY

Name of Policy: **Response to Security Incidents**
Category: **Administration and Operations**
Policy No.: **IS-25**

Review Date:

Name of Counsel: Patrick B. McDermott, Esq.

Comments of Counsel:

1. **Virginia Code Compliance:** **No violation**
2. **Federal Law Compliance:** **No violation, correct citations**
3. **Grammar and Punctuation:** **Acceptable**
4. **Comments:** **None**

Patrick B. McDermott, Esq.

Signature of Counsel

Policy and Procedures

Category: Administration and Operations

Title: Response to Security Incidents

Policy Number: IS-25

Primary Areas Affected: All

Policy and Procedures

Category:	Administration and Operations
Title:	Response to Security Incidents
Policy Number:	IS-25
Primary Areas Affected:	All

Policy Statement

Colonial Behavioral Health (CBH) will ensure that Security Incidents (defined below), including any breach of unsecured protected health information (UPHI), are identified and responded to promptly. CBH will take appropriate steps to mitigate the harmful effects of any such incident to the extent practicable.

Source of Authorization

Board of Directors

Legal/Regulatory References

HIPAA Security Rule; 42 CFR 164.308(a)(6)

Definitions

A "Security Incident" means any attempted or successful unauthorized access, use, disclosure, modification, or destruction of any electronic information, or the interference with system operations in CBH's information systems. This includes but is not limited to stolen or inappropriately obtained passwords, corrupted back-ups, viral attacks, physical break-ins, theft or loss of electronic media, or failure to properly and promptly terminate employee access.

Procedures

Any employee having knowledge of a suspected Security Incident shall immediately report the suspected incident to the CBH's Security Officer or designee via the agency's IT ticket system. Employees and workforce

Policy and Procedures

Category: Administration and Operations

Title: Response to Security Incidents

Policy Number: IS-25

Primary Areas Affected: All

members who identify any suspicious activity on CBH's electronic information systems, such as phishing attempts, suspicious emails or unauthorized access to ePHI, are required to report such activity immediately by filing an IT ticket or contacting their supervisor. If a supervisor receives a verbal report of a potential Security Incident, the supervisor must document the report in writing and share it with CBH's Security Officer.

The Security Officer or designee shall investigate the potential Security Incident and shall take immediate steps to contain and eradicate the Security Incident by securing the agency's systems and removing any on-going threats to ePHI. CBH will engage with outside IT vendors, security experts and legal counsel as necessary during the investigation and response. The Security Officer will oversee a process to determine the potential harm of the Security Incident and will take steps to prevent or mitigate any harmful effects. The Security Officer shall immediately notify CBH's senior leadership of Security Incidents that have the potential to have a material impact on ePHI.

The Security Officer shall conduct a post-incident review which will document the incident and its outcome, including steps taken to prevent or mitigate harmful effects. As part of the review, the Security Officer shall determine, if possible, the root cause of the incident, and identify any person(s) involved in or responsible for the Security Incident. In addition, the Security Officer shall document any security gaps noted during the review, and shall take steps to address the gaps, with the goal of preventing a recurrence of the same or similar Security Incident. The Security Officer shall consult with IT professionals, legal counsel, and other subject-matter experts, as necessary, during its investigation and review process.

In the event of a demonstrated Security Incident, the Security Officer shall conduct an appropriate Security Analysis and evaluate the Security Incident as a part of the Company's ongoing Risk Management program. To the extent any Security Incident also constitutes a "Breach of UPHI", the Security Officer will notify the Privacy Officer and seek legal advice and assistance in evaluating and reporting the incident, as needed.

Policy and Procedures

Category: Administration and Operations

Title: Response to Security Incidents

Policy Number: IS-25

Primary Areas Affected: All

CBH shall review and test the effectiveness of its Security Incident response plans annually, and document this review in writing. CBH will modify its Security Incident response policies and procedures as reasonable and appropriate based on this annual review.

All documentation related to Security Incidents shall be maintained for a minimum period of six (6) years. All employees are made aware of this Policy at least once a year as part of their annual training. All employees shall cooperate with the Security Officer in investigating and responding to Security Incidents.

Policy and Procedures

Category:	Administration and Operations
Title:	Response to Security Incidents
Policy Number:	IS-25
Primary Areas Affected:	All

Diary of Changes

Date of Origin

2/6/2025

Dates of Review

3/3/2026

Dates of Revision

3/3/2026

Approved By

_____	_____
Signature	Effective Date
_____	CBH Board Chair
Printed Name	Title

Action Item 8

Revision of Policy IS-26 – Contingency Plans

Background:

CBH staff have reviewed the CBH Contingency Plans Policy (Policy IS-26) and are pleased to recommend revisions to the Board of Directors for review.

IS-26 Contingency Plans policy was originally reviewed in 2025 by Liz Heddleston of Woods Rogers and the agency's lawyer, Pat McDermott.

This policy and accompanying revisions have been reviewed and approved by the agency's lawyer, Pat McDermott.

Summary of Changes:

Current Contingency Plans Policy	Proposed Changes to Policy
Old policy format	Formatted to reflect new policy template structure.
There are no other changes from the 4/2025 approved policy.	

Motion from the CBH Executive Committee:

That the Board approve the revisions to Contingency Plans policy as presented.

COLONIAL BEHAVIORAL HEALTH

COUNSEL REVIEW OF BOARD POLICY

Name of Policy: **Contingency Plans**
Category: **Administration and Operations**
Policy No.: **IS-26**

Review Date: **February 16, 2026**

Name of Counsel: Patrick B. McDermott, Esq.

Comments of Counsel:

1. **Virginia Code Compliance:** **No violation**
2. **Federal Law Compliance:** **No Violation**
3. **Grammar and Punctuation:** **Acceptable**
4. **Comments:** **Reference to Microsoft Azure 4-hour backups**

Patrick B. McDermott, Esq.

Signature of Counsel

Policy and Procedures

Category: Administration and Operations

Title: Contingency Plans

Policy Number: IS-26

Primary Areas Affected: All

Policy and Procedures

Category:	Administration and Operations
Title:	Contingency Plans
Policy Number:	IS-26
Primary Areas Affected:	All

Policy Statement

Colonial Behavioral Health (CBH) will maintain policies and procedures for responding to an emergency occurrence that damages any of CBH's systems that contain ePHI. CBH will develop a contingency plan that aims to allow the agency to return to its daily operations as quickly as possible after an unforeseen event. The plan will aim to protect agency resources and minimize disruptions to individual served. Examples of emergency occurrences covered by the contingency plan include natural disasters, such as wildfire, damaging wind, floods, hurricanes, tornadoes and earthquakes; man-made disasters, such as vandalism, cyberattacks, biochemical warfare, toxic emissions, or civil unrest/terrorism; and infrastructure issues, such as blackouts, road blocks, building hazards, network or data center outages.

Source of Authorization

Board of Directors

Legal/Regulatory References

45 CFR § 164.308(a)(7); Library of Virginia State Archival and Records Management Services Division schedule for Community Services Boards http://www.lva.virginia.gov/agencies/records/sched_local/GS-18.pdf

Definitions

N/A

Policy and Procedures

Category:	Administration and Operations
Title:	Contingency Plans
Policy Number:	IS-26
Primary Areas Affected:	All

Procedures

The following are components of CBH's contingency plan:

1. **Data Backup**

   To reduce the likelihood of data loss or corruption, CBH will create and maintain retrievable exact copies of ePHI and other data necessary for the operation of the information system. CBH information systems will have full backups performed in Microsoft Azure every 4 hours starting 8:00AM UTC for 12 hours, instant restore recovery snapshot(s) for 7 days, daily backup point retention taken every day for 30 days, and monthly backup point retention taken every month on First Sunday for 12 months. All virtual machines are configured for Azure Site Recovery as part of the Disaster Recovery/Business Continuity plan. All machines are configured to failover to the West US Datacenter, which satisfies the need for a secure location separate from the information system. This schedule is based on the potential risk of data loss or corruption and on the application and data criticality analysis. Backups will contain sufficient information to be able to restore the information system to a recent, operable, and accurate state.

   Accurate and complete records of existing backups and the location of backup media will be maintained. Backup files will be retained for an appropriate time period, based on applicable state or federal mandated retention requirements, storage considerations, and costs.

2. **Disaster Recovery Plan**

   CBH will establish, and implement as needed, procedures to restore any loss of data, including but not limited ePHI, impacted by an emergency occurrence or other unforeseen event.

Policy and Procedures

Category: Administration and Operations

Title: Contingency Plans

Policy Number: IS-26

Primary Areas Affected: All

3. **Emergency Mode Operation Plan**

   CBH will establish, and implement as needed, procedures to enable continuation of critical business processes for protection of the security of ePHI while the system that normally provides information is unavailable. CBH will have measures in place to allow users to access the agency's systems and network remotely if there no access to the physical building.

4. **Testing and Revision Procedures**

   CBH will periodically test the effectiveness of its contingency plan. This includes reviewing the contents of the contingency plan, performing tests of the plan's effectiveness and recording the results of those tests. CBH will revise its contingency plan to improve any identified gaps or deficiencies, as needed.

5. **Applications and Data Criticality Analysis**

   CBH will identify what applications and data are critical for the contingency plan. This will help the agency prioritize contingency planning and minimize loss. CBH will take into account the relative criticality of specific applications and data that may contain ePHI.

6. **Incident Response Team**

   CBH will establish an incident response team that will be responsible for leading the response to emergency incidents impacting ePHI. The team will include members from the senior leadership, the Security Officer, the outside security team, and other members as appropriate. CBH will periodically train the incident response team on their role and responsibilities.

Policy and Procedures

Category:	Administration and Operations
Title:	Contingency Plans
Policy Number:	IS-26
Primary Areas Affected:	All

Diary of Changes

Date of Origin

2/6/2025

Dates of Review

3/3/2026

Dates of Revision

3/3/2026

Approved By

_____ _____

Signature Effective Date

_____ Choose a signer.

Printed Name Title

Action Item 9

Revision of Policy IS-27 – Risk Analysis and Risk Management

Background:

CBH staff have reviewed the CBH Risk Analysis and Risk Management Policy (Policy IS-27) and are pleased to recommend revisions to the Board of Directors for review.

IS-27 Risk Analysis and Risk Management policy was originally reviewed in 2025 by Liz Heddleston of Woods Rogers and the agency's lawyer, Pat McDermott.

This policy and accompanying revisions have been reviewed and approved by the agency's lawyer, Pat McDermott.

Summary of Changes:

Current Risk Analysis and Risk Management Policy	Proposed Changes to Policy
Old policy format	Formatted to reflect new policy template structure.
There are no other changes from the 4/2025 approved policy.	

Motion from the CBH Executive Committee:

That the Board approve the revisions to Risk Analysis and Risk Management policy as presented.

COLONIAL BEHAVIORAL HEALTH

COUNSEL REVIEW OF BOARD POLICY

Name of Policy: **Risk Analysis and Risk Management**
Category: **Administration and Operations**
Policy No.: **IS-27**

Review Date: **February 16, 2026**

Name of Counsel: Patrick B. McDermott, Esq.

Comments of Counsel:

1. **Virginia Code Compliance:** **No violation**
2. **Federal Law Compliance:** **Correct Citation of 45 CFR 164.308(a)**
3. **Grammar and Punctuation:** **Acceptable**
4. **Comments:** **No recommendations**

Patrick B. McDermott, Esq.

Signature of Counsel

Policy and Procedures

Category: Administration and Operations

Title: Risk Analysis and Risk Management

Policy Number: IS-27

Primary Areas Affected: All

Policy and Procedures

Category:	Administration and Operations
Title:	Risk Analysis and Risk Management
Policy Number:	IS-27
Primary Areas Affected:	All

Policy Statement

Colonial Behavioral Health (CBH) shall conduct security risk analyses to assess the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information ("ePHI") maintained by the agency. CBH will document the findings, recommendations, and action plan resulting from the risk analysis in a written risk management plan.

Source of Authorization

Board of Directors

Legal/Regulatory References

HIPAA Security Rule; 45 CFR § 164.308(a)

Definitions

N/A

Procedures

Security Risk Assessment

The overall goal of the security risk analysis is to provide for the ongoing privacy and security of CBH's ePHI, to protect against reasonably anticipated threats or hazards to the security and integrity of the CBH's ePHI, and to ensure compliance with the HIPAA Security Rule. CBH will conduct a comprehensive security risk analysis that

Policy and Procedures

Category: Administration and Operations

Title: Risk Analysis and Risk Management

Policy Number: IS-27

Primary Areas Affected: All

meets the requirements of the HIPAA Security Rule at a frequency of at least annually. In the interim, the security risk analysis will be reviewed, and updated as needed, following the discovery of a breach of unsecured ePHI, a security incident, or in response to operational changes affecting how EPHI is processed, stored or handled.

The security risk analysis will confirm and document where CBH's ePHI is located. To that end, CBH will maintain an inventory of the agency's IT assets, and will document how ePHI moves through, into and out of CBH's information systems. As part of this process, CBH will identify and document external sources of ePHI, such as vendors or external third parties that create, receive, maintain, or transmit ePHI on behalf of CBH.

The security risk analysis will also identify reasonably anticipated threats, vulnerabilities, and risks to ePHI, as well as existing security controls to mitigate those risks. The list of threat events and threat sources should include reasonably anticipated and probable human and natural incidents that can negatively affect CBH's ability to protect ePHI (e.g., cyber attacks and weather emergencies). CBH should also develop a list of vulnerabilities (i.e., flaws or weaknesses) that could be exploited by potential threat sources. CBH should assess and document the likelihood that a threat would exploit an identified vulnerability and result in an adverse effect, and the potential impact of such threats. Each threat should be assigned a risk level (e.g., very low, low, moderate, high or very high).

Once the security risk analysis is documented, it should be shared with the senior leadership team and other stakeholders involved in CBH's risk management planning.

Risk Management Plan

The results of each risk analysis shall be documented in writing and will include recommendations for follow-up and the implementation of additional security controls, as necessary, to reduce risks and vulnerabilities to ePHI.

Policy and Procedures

Category: Administration and Operations

Title: Risk Analysis and Risk Management

Policy Number: IS-27

Primary Areas Affected: All

CBH will develop a written risk management plan to document the key findings from the security risk analysis. The risk management plan will prioritize the risk and threats identified in the security analysis based on assigned risk level and other factors.

The risk management plan will identify any measures CBH will take to mitigate identified risks, the individual(s) in charge of overseeing the mitigation measures, and the expected timeline for completion. CBH will coordinate with its internal IT team, external vendors, and/or third-party security experts, as appropriate, to deploy the security controls set forth in the risk management plan. CBH will communicate its risk management plan to workforce members and outside vendors involved in implementing CBH's risk management strategy and responding to threats or vulnerabilities to ePHI. CBH will implement and update policies, as appropriate, to address issues identified through risk analysis.

The results of all risk analyses (including the security risk analysis and risk management plan) shall be maintained as a part of the Plan's HIPAA compliance records for a period of at least six (6) years from the date of the completion of such analysis.

Policy and Procedures

Category:	Administration and Operations
Title:	Risk Analysis and Risk Management
Policy Number:	IS-27
Primary Areas Affected:	All

Diary of Changes

Date of Origin

2/6/2025

Dates of Review

3/3/2026

Dates of Revision

3/3/2026

Approved By

_____	_____
Signature	Effective Date
_____	CBH Board Chair
Printed Name	Title

Action Item 10

Revision of Policy IS-28 – Device and Asset Controls

Background:

CBH staff have reviewed the CBH Device and Asset Controls Policy (Policy IS-28) and are pleased to recommend revisions to the Board of Directors for review.

IS-28 Device and Asset Controls policy was originally reviewed in 2025 by Liz Heddleston of Woods Rogers and the agency's lawyer, Pat McDermott.

This policy and accompanying revisions have been reviewed and approved by the agency's lawyer, Pat McDermott.

Summary of Changes:

Current Device and Asset Controls Policy	Proposed Changes to Policy
Old policy format	Formatted to reflect new policy template structure.
There are no other changes from the 4/2025 approved policy.	

Motion from the CBH Executive Committee:

That the Board approve the revisions to Device and Asset Controls policy as presented.

COLONIAL BEHAVIORAL HEALTH

COUNSEL REVIEW OF BOARD POLICY

Name of Policy: **Device and Asset Control**
Category: **Administration and Operations**
Policy No.: **IS-28**

Review Date: **February 16, 2026**

Name of Counsel: Patrick B. McDermott, Esq.

Comments of Counsel:

1. **Virginia Code Compliance:** **No violation**
2. **Federal Law Compliance:** **Correct Citation: 45 CFR 164.310(d)(1)-(2)**
3. **Grammar and Punctuation:** **Acceptable**
4. **Comments:** **No recommendations**

Patrick B. McDermott, Esq.

Signature of Counsel

Policy and Procedures

Category: Administration and Operations

Title: Device and Asset Control

Policy Number: IS-28

Primary Areas Affected: All

Policy and Procedures

Category:	Administration and Operations
Title:	Device and Asset Control
Policy Number:	IS-28
Primary Areas Affected:	All

Policy Statement

Colonial Behavioral Health (CBH) will take reasonable steps to ensure the safety, integrity and confidentiality of ePHI contained on electronic devices and technology assets, such as servers, laptops, smartphones, desktops, tablets, hard drives, USB drives, CDs/DVDs, memory cards, and similar devices or assets. These measures will include appropriate procedures to protect ePHI upon receipt, installation, change in use, removal, or disposal of such devices or technology assets. For the purposes of this policy, "technology assets" refers to components of information systems, including but not limited to hardware, software, electronic media, information, and data.

Source of Authorization

Board of Directors

Legal/Regulatory References

HIPAA Security Rule, 45 CFR § 164.310(d)(1)-(2)

Definitions

N/A

Procedures

CBH will periodically identify electronic devices and technology assets that contain or provide access to ePHI and will document and store the inventory appropriately in a secure manner. To the extent applicable, the

Policy and Procedures

Category: Administration and Operations

Title: Device and Asset Control

Policy Number: IS-28

Primary Areas Affected: All

inventory will document the following information: location of device/asset, which workforce members are authorized to access or possess the device/asset, and where the device/asset is moved to. The inventory shall be updated as appropriate during the life cycle of the device or asset, including procurement, deployment, maintenance and decommissioning.

CBH will implement processes to address the disposal of devices and technology assets to ensure that all ePHI contained on such device or asset is permanently, completely and irreversibly deleted. The Security Officer, or designee, will be responsible for approval of the erasing method to be used.

CBH will implement procedures to ensure that all ePHI stored on electronic devices and technology assets is permanently removed before the device or asset is reassigned to another user, marked surplus for future use, retired or re-used in an external setting. For example, the ePHI on electronic devices and assets will be permanently erased to ensure that prior data is no longer accessible. After ePHI has been erased from a device or asset, the device or asset must be tested by the Security Officer or an authorized member of CBH's Information Technology (IT) team to ensure the ePHI has been permanently deleted before the device or asset can be re-used or disposed of.

CBH will maintain a record of the movements of electronic devices and assets and any personnel responsible for such movements. To the extent feasible, CBH will create a retrievable, exact copy of ePHI, when needed, before movement of equipment. CBH employees can only take devices containing ePHI off the property of CBH as stipulated in CBH Policy 2 – Confidentiality. Employees will not leave or store portable devices containing ePHI in their vehicles or any other unsecured location. Lost or stolen devices containing ePHI must be reported immediately to the Security Officer.

Policy and Procedures

Category:	Administration and Operations
Title:	Device and Asset Control
Policy Number:	IS-28
Primary Areas Affected:	All

Diary of Changes

Date of Origin

2/6/2025

Dates of Review

3/3/2026

Dates of Revision

3/3/2026

Approved By

_____	_____
Signature	Effective Date
_____	CBH Board Chair
Printed Name	Title

Action Item 11

Revision of Policy IS-29 – Facility Access Controls

Background:

CBH staff have reviewed the CBH Facility Access Controls Policy (Policy IS-29) and are pleased to recommend revisions to the Board of Directors for review.

IS-29 Facility Access Controls policy was originally reviewed in 2025 by Liz Heddleston of Woods Rogers and the agency's lawyer, Pat McDermott.

This policy and accompanying revisions have been reviewed and approved by the agency's lawyer, Pat McDermott.

Summary of Changes:

Current Facility Access Controls Policy	Proposed Changes to Policy
Old policy format	Formatted to reflect new policy template structure.
There are no other changes from the 4/2025 approved policy.	

Motion from the CBH Executive Committee:

That the Board approve the revisions to Facility Access Controls policy as presented.

COLONIAL BEHAVIORAL HEALTH

COUNSEL REVIEW OF BOARD POLICY

Name of Policy: **Facility Access Controls**
Category: **Administration and Operations**
Policy No.: **IS-29**

Review Date: **February 16, 2026**

Name of Counsel: Patrick B. McDermott, Esq.

Comments of Counsel:

1. **Virginia Code Compliance:** **No violation**
2. **Federal Law Compliance:** **Correct Citation: 45 CFR 164.310(a)(1)-(2)**
3. **Grammar and Punctuation:** **Acceptable**
4. **Comments:** **No recommendations**

Patrick B. McDermott, Esq.

Signature of Counsel

Policy and Procedures

Category: Administration and Operations

Title: Facility Access Controls

Policy Number: IS-29

Primary Areas Affected: All

Policy and Procedures

Category:	Administration and Operations
Title:	Facility Access Controls
Policy Number:	IS-29
Primary Areas Affected:	All

Policy Statement

Colonial Behavioral Health (CBH) will take reasonable steps to limit physical access to electronic information systems and the facilities where they are located to prevent unauthorized physical access, theft and physical damage to ePHI. The agency's physical safeguards will be designed to protect ePHI from unauthorized use while ensuring that properly authorized access is allowed.

Source of Authorization

Board of Directors

Legal/Regulatory References

HIPAA Security Rule, 45 CFR § 164.310(a)(1)-(2)

Definitions

N/A

Procedures

Steps to limit physical access to ePHI may include:

a. Safeguarding the exterior and interior of the facility with reasonable measures, such as locks, surveillance cameras, alarms or other access control devices;

b. Implementing methods for monitoring and verifying facility access authorizations;

Policy and Procedures

Category: Administration and Operations

Title: Facility Access Controls

Policy Number: IS-29

Primary Areas Affected: All

c. Validating a person's access to facilities based on their role or function, including visitor management;

d. Safeguarding equipment contained within facilities and on the premises to protect ePHI and prevent unauthorized access to ePHI to the degree possible;

e. Documenting repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors and locks);

f. Establishing procedures to allow facility access in support of the restoration of lost data in the event of an emergency; or

In the event that fire codes prevent these areas from being locked, the doors will be kept closed to reduce traffic to a minimum.

Policy and Procedures

Category:	Administration and Operations
Title:	Facility Access Controls
Policy Number:	IS-29
Primary Areas Affected:	All

Diary of Changes

Date of Origin

2/6/2025

Dates of Review

3/3/2026

Dates of Revision

3/3/2026

Approved By

_____	_____
Signature	Effective Date
_____	CBH Board Chair
Printed Name	Title

Action Item 12

Revision of Policy IS-30 – Malicious Software Protection

Background:

CBH staff have reviewed the CBH Malicious Software Protection Policy (Policy IS-30) and are pleased to recommend revisions to the Board of Directors for review.

IS-30 Malicious Software Protection policy was originally reviewed in 2025 by Liz Heddleston of Woods Rogers and the agency's lawyer, Pat McDermott.

This policy and accompanying revisions have been reviewed and approved by the agency's lawyer, Pat McDermott.

Summary of Changes:

Current Malicious Software Protection Policy	Proposed Changes to Policy
Old policy format	Formatted to reflect new policy template structure.
There are no other changes from the 4/2025 approved policy.	

Motion from the CBH Executive Committee:

That the Board approve the revisions to Malicious Software Protection policy as presented.

COLONIAL BEHAVIORAL HEALTH

COUNSEL REVIEW OF BOARD POLICY

Name of Policy: **Malicious Software Protection**
Category: **Administration and Operations**
Policy No.: **IS-30**

Review Date: **February 16, 2026**

Name of Counsel: Patrick B. McDermott, Esq.

Comments of Counsel:

1. **Virginia Code Compliance:** **No violation**
2. **Federal Law Compliance:** **Correct Citation: 45 CFR 64.308(a)(5)(ii)(B)**
3. **Grammar and Punctuation:** **Acceptable**
4. **Comments:** **No recommendations**

Patrick B. McDermott, Esq.

Signature of Counsel

Policy and Procedures

Category: Administration and Operations

Title: Malicious Software Protection

Policy Number: IS-30

Primary Areas Affected: All

Policy and Procedures

Category:	Administration and Operations
Title:	Malicious Software Protection
Policy Number:	IS-30
Primary Areas Affected:	All

Policy Statement

Colonial Behavioral Health (CBH) will ensure that the ePHI created or maintained by CBH is reasonably protected from corruption by malicious software (malware) of any origin. For the purposes of this policy, "malicious software" refers to software or firmware intended to perform an unauthorized action or activity that will have an adverse impact on an electronic information system and and/or the confidentiality, integrity or availability of ePHI. Examples include but are not limited to viruses, worms, Trojan horses, spyware, and some forms of adware.

Source of Authorization

Board of Directors

Legal/Regulatory References

HIPAA Security Rule, 45 CFR 164.308(a)(5)(ii)(B)

Definitions

N/A

Procedures

CBH shall develop and implement specific procedures to prevent, detect and report the presence of malicious software within the agency's computer networks and information systems. Such policies and procedures include but are not limited to:

Policy and Procedures

Category: Administration and Operations

Title: Malicious Software Protection

Policy Number: IS-30

Primary Areas Affected: All

a. Employees shall not receive and download files and other materials from unknown sources;

b. Employees shall not load unauthorized files or programs on company hardware;

c. Employees shall not access non-work-related internet sites on company hardware;

d. CBH shall install and maintain firewalls, virus detection and protection programs and similar electronic and hardware protections. CBH will coordinate with its external IT and security vendors to ensure that each endpoint in the agency is equipped with anti-virus software that is configured to update automatically.

e. Employees shall immediately report suspected malicious software by submitting an IT ticket and/or contacting their supervisor in accordance with IS Policy 25 – Response to Security Incidents.

f. Employees shall not have administrator-level access rights to their own devices (laptops, desktops, etc.).

Policy and Procedures

Category:	Administration and Operations
Title:	Malicious Software Protection
Policy Number:	IS-30
Primary Areas Affected:	All

Diary of Changes

Date of Origin

2/6/2025

Dates of Review

3/3/2026

Dates of Revision

3/3/2026

Approved By

_____	_____
Signature	Effective Date
_____	CBH Board Chair
Printed Name	Title

Action Item 13

Revision of Policy IS-31 – Password Management and Log-in Monitoring

Background:

CBH staff have reviewed the CBH Password Management and Log-in Monitoring Policy (Policy IS-31) and are pleased to recommend revisions to the Board of Directors for review.

IS-31 Password Management and Log-in Monitoring policy was originally reviewed in 2025 by Liz Heddleston of Woods Rogers and the agency's lawyer, Pat McDermott.

This policy and accompanying revisions have been reviewed and approved by the agency's lawyer, Pat McDermott.

Summary of Changes:

Current Password Management and Log-in Monitoring Policy	Proposed Changes to Policy
Old policy format	Formatted to reflect new policy template structure.
There are no other changes from the 4/2025 approved policy.	

Motion from the CBH Executive Committee:

That the Board approve the revisions to Password Management and Log-in Monitoring policy as presented.

COLONIAL BEHAVIORAL HEALTH

COUNSEL REVIEW OF BOARD POLICY

Name of Policy: **Password Management and Log-in Monitoring**
Category: **Administration and Operations**
Policy No.: **IS-31**

Review Date: **February 16, 2026**

Name of Counsel: Patrick B. McDermott, Esq.

Comments of Counsel:

1. **Virginia Code Compliance:** **No violation**
2. **Federal Law Compliance** **45 CFR 164.308(a)(5)(ii)(C)-(D)**
3. **Grammar and Punctuation:** **Acceptable**
4. **Comments:** **No recommendations**

Patrick B. McDermott, Esq.

Signature of Counsel

Policy and Procedures

Category: Administration and Operations

Title: Password Management and Log-in Monitoring

Policy Number: IS-31

Primary Areas Affected: All

Policy and Procedures

Category:	Administration and Operations
Title:	Password Management and Log-in Monitoring
Policy Number:	IS-31
Primary Areas Affected:	All

Policy Statement

For all systems containing ePHI, Colonial Behavioral Health (CBH) will implement procedures for monitoring log-in attempts and for managing and safeguarding passwords.

Source of Authorization

Board of Directors

Legal/Regulatory References

45 CFR § 164.308(a)(5)(ii)(C) – (D)

Definitions

N/A

Procedures

Password Management

CBH will protect the confidentiality of workforce member passwords that grant access to the agency's information systems that contain ePHI. To that end, CBH will implement procedures for creating, changing and safeguarding passwords that allow access to ePHI. These password procedures shall, at a minimum, specify the number and nature of characters required and the frequency of required changes.

Policy and Procedures

Category: Administration and Operations

Title: Password Management and Log-in Monitoring

Policy Number: IS-31

Primary Areas Affected: All

All workforce members of CBH are required to safeguard their passwords. Workforce members are prohibited from posting passwords anywhere on or near the workstation, "lending" passwords to any other employee or third party for convenience or any other reason, or otherwise sharing passwords with any other employee or third party. Employees should create account passwords for CBH that are different from the ones used for personal internet or email access (e.g., Gmail, Yahoo, Facebook, etc.)

CBH's network requires all employees to change their login password every **90 days** and will not allow access until the password change is complete. For additional details about CBH's current password requirements and safeguards, see **IS-20 General Technical Safeguards and Access Controls.**

Log-In Monitoring

CBH will implement a process for monitoring log-in attempts to information systems that contain ePHI and reporting suspicious activity or log-in discrepancies. CBH will deploy technical controls that disable or suspend the access of a user to relevant electronic information systems after a pre-determined number of unsuccessful authentication attempts. CBH's assigned 24x7 security vendor will review log-in monitoring process to ensure that it is effective. CBH will include external Information Technology (IT) and applicable security vendor in CBH's periodic review of log-in monitoring processes as appropriate.

Policy and Procedures

Category:	Administration and Operations
Title:	Password Management and Log-in Monitoring
Policy Number:	IS-31
Primary Areas Affected:	All

Diary of Changes

Date of Origin

2/6/2025

Dates of Review

3/3/2026

Dates of Revision

3/3/2026

Approved By

_____	_____
Signature	Effective Date
_____	CBH Board Chair
Printed Name	Title

Action Item 14

Revision of Policy IS-32 Transmission Security Guidelines

Background:

CBH staff have reviewed the CBH Transmission Security Guidelines Policy (Policy IS-32) and are pleased to recommend revisions to the Board of Directors for review.

IS-32 Transmission Security Guidelines policy was originally reviewed in 2025 by Liz Heddleston of Woods Rogers and the agency's lawyer, Pat McDermott.

This policy and accompanying revisions have been reviewed and approved by the agency's lawyer, Pat McDermott.

Summary of Changes:

Current Transmission Security Guidelines Policy	Proposed Changes to Policy
Old policy format	Formatted to reflect new policy template structure.
There are no other changes from the 4/2025 approved policy.	

Motion from the CBH Executive Committee:

That the Board approve the revisions to Transmission Security Guidelines policy as presented.

COLONIAL BEHAVIORAL HEALTH

COUNSEL REVIEW OF BOARD POLICY

Name of Policy: **Transmission Security Guidelines**
Category: **Administration and Operations**
Policy No.: **IS-32**

Review Date: **February 16, 2026**

Name of Counsel: Patrick B. McDermott, Esq.

Comments of Counsel:

1. **Virginia Code Compliance:** **No violation**

2. **Federal Law Compliance** **45 CFR 164.312(e)(1)**
   45 CFR 164.312(e)(2)(1)-(ii)

3. **Grammar and Punctuation:** **Acceptable**

4. **Comments:** **Add: 45 CFR 164.304 where 'encryption" is defined in this policy.**

Patrick B. McDermott, Esq.

Signature of Counsel

Policy and Procedures

Category: Administration and Operations

Title: Transmission Security Guidelines

Policy Number: IS-32

Primary Areas Affected: All

Policy and Procedures

Category:	Administration and Operations
Title:	Transmission Security Guidelines
Policy Number:	IS-32
Primary Areas Affected:	All

Policy Statement

Colonial Behavioral Health (CBH) will implement reasonable and appropriate security measures to protect against unauthorized access to ePHI transmitted over an electronic communications network. All CBH applications that transfer ePHI over an electronic communications network (e.g., email, file transfer, web browser) are subject to this Policy. CBH will identify and document all methods used to transmit ePHI across the organization and will periodically review and update this documentation to ensure it is up to date.

Source of Authorization

Legal/Regulatory References

45 CFR § 164.312(e)(1); 45 § CFR 164.312(e)(2)(i)-(ii)

Definitions

1. **Access** is defined as "the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource."
2. **Encryption** is defined as: "the use of an algorithmic process to transfer data into a form in which there is a low probability of assigning meaning without use of a confidential process or key and such confidential process or key that might enable decryption has not been breached."
    a. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The

Policy and Procedures

Category: Administration and Operations

Title: Transmission Security Guidelines

Policy Number: IS-32

Primary Areas Affected: All

encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.

b. Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

Procedures

1. **Appropriate Transmission of ePHI**: ePHI may only be transmitted in accordance with CBH's policies governing the use and disclosure of PHI. See Policy 40 – Electronic Protected Health Information.
2. **Electronic Transmissions of ePHI to networks outside of CBH's network (including cloud-based systems)**: To appropriately guard against the unauthorized acquisition, access, use or disclosure of data that is being transmitted from CBH's network to a network outside of CBH, the procedures outlined in this Policy must be implemented and complied with by all CBH workforce members.
    a. All transmissions of ePHI from the CBH's network to an outside network must be administratively approved by the agency's Director of Information Services prior to transmission. If approved, the transmission must include additional security measures that use an encryption mechanism between the sending and receiving entities, and the files or documents containing ePHI must be encrypted before transmission

Policy and Procedures

Category: Administration and Operations

Title: Transmission Security Guidelines

Policy Number: IS-32

Primary Areas Affected: All

b. If approved, prior to transmitting ePHI from CBH's network to an outside network, the receiving person or entity must be authenticated, meaning that the identity of the receiving person or entity has been verified.

c. If approved, all transmissions of ePHI from CBH's network to an outside network should include only the minimum amount of information necessary.

d. If approved, for transmission of ePHI from CBH's network to an outside network using an email or messaging system, see Section 3 below.

3. **Transmissions of ePHI Using Email or Messaging Systems**

a. The transmission of ePHI from CBH to a recipient via email or other messaging system is permitted only by the agency's Director of Information Services as well as through an agency approved and supported secure email or messaging solution. Employees are prohibited from using their personal email accounts to transmit ePHI.

b. The transmission of ePHI from CBH to an outside entity via an encrypted email or messaging system is permitted only if the agency's Director of Information Services has approved the transmission. The Director of Information Services may approve certain categories of transmission that are permissible, such as messaging though the agency's EHR-based messaging system for business-related purposes. Such approved categories of transmissions will be documented in writing and communicated to the workforce on a periodic basis. Prior to the transmission, the sender must ensure that the following conditions are met:

i. The receiving entity has been authenticated.

ii. The receiving entity is aware of the transmission and is ready to receive said transmission.

Policy and Procedures

Category: Administration and Operations

Title: Transmission Security Guidelines

Policy Number: IS-32

Primary Areas Affected: All

4. **Working with ePHI outside CBH's network (working from home, while traveling, from an alternate location, etc.)**

    a. When outside CBH's network, users must log in to the VPN solution prior to working with ePHI. VPN establishes an encrypted end-to-end connection with CBH's network, preventing inappropriate access to any data moving between the user's device and CBH's network.

5. **Integrity Controls**

    a. CBH will implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of. CBH will use network communication protocols and other methods to ensure that ePHI sent electronically is the same as the ePHI received. CBH will coordinate with its Information Services department and outside IT vendors as necessary to ensure that adequate integrity controls are in place.

Policy and Procedures

Category:	Administration and Operations
Title:	Transmission Security Guidelines
Policy Number:	IS-32
Primary Areas Affected:	All

Diary of Changes

Date of Origin

2/6/2025

Dates of Review

3/3/2026

Dates of Revision

3/3/2026

Approved By

_____	_____
Signature	Effective Date
_____	CBH Board Chair
Printed Name	Title

Recruitment Status
January 15, 2026 – February 11, 2026

For the period of January 15, 2026, through February 11, 2026, Colonial Behavioral Health (CBH) successfully completed 7 hires (all full-time positions), and the agency has one additional full-time offer in a pending status. Pending acceptance of position, the agency will be recruiting 25 positions which include 19 full-time positions, two (2) part-time positions and four (4) PRN/WAR positions. CBH experienced 5 resignations (all full-time positions) during the reporting period and one (1) orientation no-show.

Colonial Behavioral Health
Wellness, Support & Recovery Services

YEAR TO DATE REVENUES AND EXPENDITURES
as of
January 31, 2026

REVENUE

CATEGORY	TOTAL BUDGET	RECEIVED YTD	BUDGET YTD	% RECEIVED	ACTUAL YTD vs BUDGET YTD
State	$ 14,274,982	$ 7,592,351	$ 8,327,073	91%	$ (734,721)
Local	$ 4,147,000	2,363,917	2,419,083	98%	$ (55,167)
Fees	$ 6,421,285	3,686,633	3,745,750	98%	$ (59,117)
Grants/Other	$ 736,943	1,280,579	429,884	298%	$ 850,695
Total Revenue	$ 25,580,210	$ 14,923,480	$ 14,921,789	100%	$ 1,691

FY26 EXPENDITURES

CATEGORY	TOTAL BUDGET	EXPENDED YTD	BUDGET YTD	% EXPENDED	ACTUAL YTD vs BUDGET YTD
Personnel	$ 19,181,019	$ 10,164,002	$ 11,065,972	92%	$ 901,971
Staff Development	$ 116,497	81,645	67,956	120%	(13,689)
Facility	$ 1,776,594	810,585	1,036,346	78%	225,761
Equipment and Supplies	$ 1,509,307	566,223	880,429	64%	314,207
Transportation	$ 189,408	63,600	110,488	58%	46,888
Consultant and Contractual	$ 2,549,955	1,132,770	1,487,474	76%	354,704
Client Supports	$ 87,348	37,420	50,953	73%	13,532
Miscellaneous	$ 170,083	106,865	99,215	108%	(7,650)
Total Expenditures	$ 25,580,210	$ 12,963,110	$ 14,798,834	88%	$ 1,835,724

Operating Margin	$ -	$ 1,960,370

Unless noted otherwise, all amounts are modified cash basis: revenues recognized when earned and received; expenditures upon disbursement

1/31/26 Cash Balance	$ 15,448,418

CRISIS SERVICES CENTER PROJECT

CATEGORY	PROJECT BUDGET	PROJECT TO DATE
DBHDS Grant	$ 12,000,000	$ 4,200,684
Interest Earned		$ 8,656
Total Revenue	$ 12,000,000	$ 4,209,340
Personnel		$ 114,992
Mileage		$ 500
Consultant and Contractual		$ 3,300,705
Miscellaneous		$ 243
Total Expenditures		$ 3,416,440

COLONIAL BEHAVIORAL HEALTH
Executive Director's Report – March 2026

Agency Issues

1. Center for Support & Wellness construction was slowed by lingering ice at the site, but our partners (the Henderson team) are working to keep the project on schedule.
2. We have posted the Notice to Award for the Phase 2 RFP selecting Henderson, Inc. as the team with which we will work to negotiate an Interim Agreement under PPEA.
3. The VACSB Annual Training Conference will be held May 6-8 in Richmond. If you are interested in attending, please contact Kristy Wallace to manage your registration.
4. York County's Financial Services staff are serving as invaluable support for our Finance staff. This is particularly important as we are working to develop the FY27 budget in time for the Board to review the draft budget in May.
5. We are pleased to announce that Ms. Sherri Ousey is scheduled to begin employment as our new Director of Finance, effective 3/16/2026. We are very excited about the experience, skills, and enthusiasm she brings to CBH at this important time.
    a. Particular recognition is due to Susan Goodwin for her invaluable role in this process. She dedicated a great deal of time to this role for our benefit.

Community Issues

1. Licensed Child & Adolescent Therapist Casandra Jones is presenting a workshop at the American Group Psychotherapy Association (AGPA) conference on March 5th. The workshop is entitled *An Introduction to Tabletop Role Play Games (TT-RPG) as a Group Therapy Modality*. The workshop will utilize the game *Dungeons & Dragons*.
2. We are currently presenting CBH's work to each locality's governing bodies. We have presented (or are scheduled to present) as follows:
    a. February 9 7:00 PM Poquoson City Council
    b. February 12 2:00 PM Williamsburg City Council
    c. February 24 1:00 PM JCC Board of Supervisors
    d. March 3 6:00 PM York County Board of Supervisors

Public Policy

1. It appears that the $10 million budget amendments submitted by Senator McDougle and Delegate Anderson were not included in the Senate or House committee budget reports. These were intended to support Phase 2 of our facility expansion project.
2. A summary of State Budget actions taken to date in the 2026 Regular Session of the General Assembly will be shared as soon as details are available on the GA website.
3. We are rapidly approaching the April 1st deadline for Virginia's SAMHSA application for inclusion in the CCBHC Demonstration Program, a 10-year goal of the CSB system and many at DBHDS as well. Our Association is partnering with the National Council for Mental Wellbeing to assist the state with the application.

Respectfully submitted,
David A. Coe