WCCHS Regular Board of Managers (BOMs) Meeting January 27, 2026

The regular meeting of the Wyoming County Community Health System (WCCHS) Board of Managers, Wyoming County, New York was held on Tuesday, January 27, 2026.

CALL MEETING TO ORDER
President Kosmerl called the meeting to order at 4:00pm.

INTRODUCE/WELCOME JERRY DAVIS
President Kosmerl introduced Jerry Davis, as a new member on the WCCHS Board of Managers. Jerry previously served as Supervisor, Town of Covington and was appointed the Chairman, Wyoming County Board of Supervisors in 2020.

CONGRATULATIONS
President Kosmerl extended congratulations to Jim Brick on his appointment as Chairman, Wyoming County Board of Supervisors and Susan May on her appointment as Vice Chairman and extended an invitation to Susan to attend the BOM meetings.

ROLL CALL AND QUORUM
BOARD OF MANAGERS PRESENT/ABSENT

★ participated remotely

☒ Salman Abbasey, MD	☒ Rich Kosmerl	☒ Larry Rogers
☒ Jerry Davis	☒ Steve Perkins	☐ Janice Shirley
☒ Bryan Kehl (BOS member) at 4:05pm	☒ J. Thomas Reagan, MD	☒ James Wawrzyniak, DC ★

STAFF PRESENT/ABSENT

★ participated remotely

☒ Justin Bayliss (NF Administrator)	☒ Jeff Perry (Chief Executive Officer)
☒ Dan Farberman (WC Human Resource Director)	☒ Pam Pettnot (Executive Assistant)
☒ Mandip Panesar, MD (Hospital Medical Director) ★	☒ Mark Wright (Chief Financial Officer)

OTHERS PRESENT: Jim Brick (Chairman, Wyoming County Board of Supervisors and Supervisor, Town of Perry), Tonya Beardsley (Manager of Health Information Management and Quality/Risk Management), and Scott Schrader (County Administrator)

President Kosmerl declared that a quorum was physically present. Manager Wawrzyniak participated remotely from 1681 4th Ct., Vero Beach, FL as indicated in the meeting notice; therefore, he was counted toward the quorum and was eligible to vote.

WCCHS-26-001 ADOPT THE AGENDA
Motion by Manager Perkins and seconded by Manager Wawrzyniak, the BOM hereby adopts the agenda as presented and verbally modified to include the BOM's intent to enter into an executive session by means of a vote to be taken during the meeting.

The motion was passed upon the following vote:

VOTE								
Salman Abbasey, MD	X	Yes		No		Abstain		Absent
Jerry Davis	X	Yes		No		Abstain		Absent
Bryan Kehl		Yes		No		Abstain	X	Absent
Rich Kosmerl	X	Yes		No		Abstain		Absent
Steve Perkins	X	Yes		No		Abstain		Absent
J. Thomas Reagan, MD	X	Yes		No		Abstain		Absent
Larry Rogers	X	Yes		No		Abstain		Absent
Janice Shirley	X	Yes		No		Abstain		Absent
James Wawrzyniak, DC	X	Yes		No		Abstain		Absent
VOTE TOTAL:	8	Yes	0	No	0	Abstain	1	Absent
RESULTS	**X**	**PASS**				**FAIL**		

At 4:05pm, Manager Kehl entered the meeting during the below agenda item.

ANNUAL CORPORATE COMPLIANCE EDUCATION

Tonya Beardsley made a presentation to attendees about the WCCHS corporate compliance program – to ensure ethical standards and regulatory adherence – prevent and detect fraud, abuse, waste, and improper expenditures and promote high-quality patient care. The presentation included objectives, definitions, OIG vs OMIG, seven elements of an effective compliance program, OMIG compliance program requirements, work plan, reporting mechanisms and communication channels, responding to compliance issues, role of leadership in compliance, and cornerstone of the corporate compliance program. A copy of the presentation is on file in Administration.

WCCHS-26-002 CONSENT AGENDA

Motion by Manager Rogers and seconded by Manager Perkins, the following items were listed for consideration on the consent agenda and are hereby approved as included in the agenda packet and on file in Administration:

- BOM meeting minutes – December 16, 2025

The motion was passed upon the following vote:

VOTE								
Salman Abbasey, MD	X	Yes		No		Abstain		Absent
Jerry Davis	X	Yes		No		Abstain		Absent
Bryan Kehl	X	Yes		No		Abstain		Absent
Rich Kosmerl	X	Yes		No		Abstain		Absent
Steve Perkins	X	Yes		No		Abstain		Absent
J. Thomas Reagan, MD	X	Yes		No		Abstain		Absent
Larry Rogers	X	Yes		No		Abstain		Absent
Janice Shirley	X	Yes		No		Abstain		Absent
James Wawrzyniak, DC	X	Yes		No		Abstain		Absent
VOTE TOTAL:	9	Yes	0	No	0	Abstain	0	Absent
RESULTS	**X**	**PASS**				**FAIL**		

Motion by Manager Wawrzyniak and seconded by Manager Shirley, the following items were listed for consideration on the consent agenda and are hereby accepted as included in the agenda packet and on file in Administration:

- Leadership: Organization updates
- Accounts payable exception list
- Accounts payable report
- Write-off, denied and bad debt amounts report
- Personnel requisitions in process report
- Personnel changes/financial impact report
- Contracts and/or grants
- Medical Exec, peer review report
- Credentials committee
- Medical leave summary
- Financial statements with operational stats_
- Satisfaction surveys
- Medical staff appointments

CONTRACTS FULLY EXECUTED SINCE DECEMBER 16, 2025 BOM MEETING

Contractor Legal Name	Name of Contract	Contract Purpose	Start Date	Autorenewal?	Expiration Date	Contract Amount	NOTES
Medical Information Technology, Inc. (MEDITECH)	Health Care Information System Software Subscription Agreement and Order	MEDITECH Expanse electronic health record	12/30/2026	Yes		$1,763,760, plus one-time implementation fee of $420,000	
Ball PA, Brittany	Provider Employment Agreement Amendment #1	To provide Physician Assistant services to Primary Care	1/19/2026	Yes		$135,000 per year base compensation, plus stipend in the amount of $500 per full clinic day when working extra shifts, plus stipend for a quarterly production bonus (wRVUs), plus stipend upto $5,000 per calendar year for quality and service bonus	Moving the start date only
WCJW Radio	Radio Advertising Agreement	Radio advertising	1/1/2026	No	12/31/2026	$10,800 per year	
Medical Gas Technologies, inc.	Agreement	Annual medical gas system inspections and vacuum pump and compressor preventive maintenance	1/1/2026	No	12/31/2026	$3,600 per year	
B. J. Buirhead Co., Inc.	Preventive Maintenance Service Agreement	Maintenance service on all boilers in the health system, routine service on all parts, inspections, and replacement of gaskets, cleaning.	1/1/2026	No	12/31/2028	$13,150 per year	
Wyoming County (Inter Departmental)	Various Inpatient and Jail Behaviral Health Services	Inpatient and jail-based behavioral health services. Increase in state aid for COLAs for direct staff	1/1/2026	No	12/31/2026	Reimbursement to WCCHS; $305,987 revenue	
Gomez MD, Joseph	Physician Employment Agreement	To provide cardiology services at the hospital	1/1/2026	Yes		Base compensation $615,000, plus stipend in the amount of $1,000 per 8-hour for extra shifts, plus stipend in the amount of $70 per wRVU above base salary, plus stipend up to $10,000 per calendar year for quality and service bonus if certain criteria are met	
Nuance Communications, Inc.	Renewal order form for Clintegrity software products	Solventum, formerly 3M Health Care, eAPG State Grouper for Nuance Clintegrity Coding and Compliance Solution	1/1/2026	No	12/31/2026	$21,454 per year	
Nuance Communications, Inc.	Renewal order form for Clintegrity software products	Solventum, formerly 3M Health Care, APR-DRG State Grouper for Nuance Clintegrity Coding and Compliance Solution	1/1/2026	No	12/31/2026	$17,833 per year	
Gomez MD, Joseph	Employment Agreement - Amendment #2	To provide cardiology services at the hospital	12/22/2025	No	2/1/2027	$525,000 per year plus stipend for wRVUs	wRVUs for time period 08/01/2025 - 12/31/2025 will be paid at $64 for any wRVU over 3,333.
Grand Canyon University	Canyon Healthcare Education Collaborative Agreement	To participate in the Canyon Healthcare Education Collaborative (CHEC) program that provides WCCHS employees, spouses, and dependents a discount off tuition	12/22/2025	Yes		$0.00	
The School of Nursing of the University of Rochester	Memorandum of Agreement for Clinical Experience	To provide clinical training and experience to the students of the University	12/15/2025	No	12/31/2031	$0.00	
Becton, Dickinson and Company	BD Acquisition Agreement	Blood culture analyzer equipment and service contract renewal	12/8/2025	No	12/8/2030	$129,030.61 for 5 year term	
Prusak, Megan	Provider Employment Agreement - Amendment #1	To provide services to the residents of the service area	12/8/2025	Yes		$135,000 per year base compensation, plus stipend in the amount of $500 per eight (8) hour shift for additional shifts in various clinics, plus stipend for a quarterly production bonus (wRVUs), plus stipend upto $5,000 per calendar year for quality and service bonus, plus hospital agrees to reimburse employee up to $7,000 for RNFA certification	
American College of Radiology	Practice Site Accreditatino Survey Agreement	Survey of quality of certain radiological services	12/3/2025	No		Nonrefundable fee based upon the number of diagnostic modalities being reviewed	
Institute for Healthcare Improvement	Subaward Agreement	Grant funded for CareFront Project to be implemented by the IHI, we will receive 3 payments and up to 45,000 to participate in the CareFront Project	12/1/2025	No	10/31/2026	Revenue, $45,000	
ScreenPoint Medical, Inc.	Transpara Detection Module Subscription	AI software used by Radiologist to aid in diagnosting breast cancer when reading mammography	9/15/2025	No	9/14/2030	$4,560 per year	
ComSource, Inc.	DeepSeas statement of work cybersecurity services	Cybersecurity defense program, virtual chief information security officer advisory	4/1/2025	No	3/31/2026	$52,200	

The motion was passed upon the following vote:

VOTE								
Salman Abbasey, MD	X	Yes		No		Abstain		Absent
Jerry Davis	X	Yes		No		Abstain		Absent
Bryan Kehl	X	Yes		No		Abstain		Absent
Rich Kosmerl	X	Yes		No		Abstain		Absent
Steve Perkins	X	Yes		No		Abstain		Absent
J. Thomas Reagan, MD	X	Yes		No		Abstain		Absent
Larry Rogers	X	Yes		No		Abstain		Absent
Janice Shirley	X	Yes		No		Abstain		Absent
James Wawrzyniak, DC	X	Yes		No		Abstain		Absent
VOTE TOTAL:	9	Yes	0	No	0	Abstain	0	Absent
RESULTS	**X**	**PASS**				**FAIL**		

DISCUSSION ITEMS

MEDICAL DIRECTOR COMMENTS

Dr. Panesar reported that Dr. Reagan asked him to look into a potential quality improvement initiative related to documentation. He will follow up on this.

At 4:45pm, Manager Kehl left the meeting during the below agenda item.
At 4:46pm, Manager Kehl returned to the meeting.

QUARTERLY FINANCIAL REPORT WITH OPERATIONAL STATS

Mark Wright reported on the operating statement, benchmark summary, hospital volumes, and clinic volumes.

WCCHS-26-003 PERMISSION TO DECLARE ITEMS AS SURPLUS

Motion by President Kosmerl and seconded by Manager Shirley, the list of items presented and below be hereby approved as excess equipment and declared as surplus. The CEO is authorized to dispose of the property in a manner that serves the best interests of the public and ensures the best possible return, including but not limited to: accepting the highest purchase offer, transferring items to other Wyoming County departments, transferring to other facilities, or disposing of the items, as appropriate.

Dietary Equipment (SNF) List to Be Salvaged					
Item #	**Description**	**Brand / Model #**	**Quantity**	**Value per unit**	**Total Value**
114.1	Stainless Steel Dish Tables	Advance Tabco / DTC-S30-60R	3		
116.1	AM Select Dishwasher	Hobart / F-40078	3		
117	Adjustable Polymer "poker chip" Dish Dolly	Metro / PCDIIA	4		
112	Roll-In & Roll-Thru Refrigerator	Continental / DL2RI-SS	3		

The motion was passed upon the following vote:

VOTE								
Salman Abbasey, MD	X	Yes		No		Abstain		Absent
Jerry Davis	X	Yes		No		Abstain		Absent
Bryan Kehl	X	Yes		No		Abstain		Absent
Rich Kosmerl	X	Yes		No		Abstain		Absent
Steve Perkins	X	Yes		No		Abstain		Absent
J. Thomas Reagan, MD	X	Yes		No		Abstain		Absent
Larry Rogers	X	Yes		No		Abstain		Absent
Janice Shirley	X	Yes		No		Abstain		Absent
James Wawrzyniak, DC	X	Yes		No		Abstain		Absent
VOTE TOTAL:	9	Yes	0	No	0	Abstain	0	Absent
RESULTS	**X**	**PASS**				**FAIL**		

WCCHS-26-004 CYBERSECURITY POLICY

Motion by Manager Wawrzyniak and seconded by Manager Abbasey, the BOM hereby approves and recommends the implementation of the WCCHS Cybersecurity Policy titled *Written Information Security Policy (WISP)*, Rev. 0, as amended and attached, in accordance with the requirements set forth under 10 NYCRR § 405.46 (New York State Department of Health – Hospital Cybersecurity Requirements).

The motion was passed upon the following vote:

VOTE								
Salman Abbasey, MD	X	Yes		No		Abstain		Absent
Jerry Davis	X	Yes		No		Abstain		Absent
Bryan Kehl	X	Yes		No		Abstain		Absent
Rich Kosmerl	X	Yes		No		Abstain		Absent
Steve Perkins	X	Yes		No		Abstain		Absent
J. Thomas Reagan, MD	X	Yes		No		Abstain		Absent
Larry Rogers	X	Yes		No		Abstain		Absent
Janice Shirley	X	Yes		No		Abstain		Absent
James Wawrzyniak, DC	X	Yes		No		Abstain		Absent
VOTE TOTAL:	9	Yes	0	No	0	Abstain	0	Absent
RESULTS	**X**	**PASS**				**FAIL**		

WCCHS-26-005 DESIGNATE CHIEF INFORMATON SECURITY OFFICER

Motion by Manager Rogers and seconded by Manager Abbasey, the BOM hereby designates the *WCCHS Director of Healthcare Information Systems* as the Chief Information Security Officer (CISO), effective immediately, in accordance with 10 NYCRR § 405.46(e) (New York State Department of Health – Hospital Cybersecurity Requirements).

The motion was passed upon the following vote:

VOTE								
Salman Abbasey, MD	X	Yes		No		Abstain		Absent
Jerry Davis	X	Yes		No		Abstain		Absent
Bryan Kehl	X	Yes		No		Abstain		Absent
Rich Kosmerl	X	Yes		No		Abstain		Absent
Steve Perkins	X	Yes		No		Abstain		Absent
J. Thomas Reagan, MD	X	Yes		No		Abstain		Absent
Larry Rogers	X	Yes		No		Abstain		Absent
Janice Shirley	X	Yes		No		Abstain		Absent
James Wawrzyniak, DC	X	Yes		No		Abstain		Absent
VOTE TOTAL:	9	Yes	0	No	0	Abstain	0	Absent
RESULTS	**X**	**PASS**				**FAIL**		

EXECUTIVE SESSION

Motion by President Kosmerl and seconded by Manager Davis, for the Board to enter into executive session to discuss the following topic(s) at 4:57pm. Jeff Perry, Jim Brick, Dan Farberman, Scott Schrader, and Pam Pettnot remained. All other attendees left the meeting room.

1. Risk/accreditation/regulatory report
2. Continuous strategic plan update
3. Performance of a particular employee – CEO annual evaluation

The motion was passed upon the following vote:

VOTE								
Salman Abbasey, MD	X	Yes		No		Abstain		Absent
Jerry Davis	X	Yes		No		Abstain		Absent
Bryan Kehl	X	Yes		No		Abstain		Absent
Rich Kosmerl	X	Yes		No		Abstain		Absent
Steve Perkins	X	Yes		No		Abstain		Absent
J. Thomas Reagan, MD	X	Yes		No		Abstain		Absent
Larry Rogers	X	Yes		No		Abstain		Absent
Janice Shirley	X	Yes		No		Abstain		Absent
James Wawrzyniak, DC	X	Yes		No		Abstain		Absent
VOTE TOTAL:	9	Yes	0	No	0	Abstain	0	Absent
RESULTS	**X**	**PASS**				**FAIL**		

At 5:54pm, Scott Schrader left the meeting.
At 6:23pm, Jim Brick left the meeting.
At 6:51pm, Manager Rogers left Executive Session and returned at 6:53pm.
At 6:55pm, Manager Davis left Executive Session and returned at 6:58pm.
At 7:00pm, Manager Abbasey left Executive Session and returned at 7:02pm.
At 7:05pm, Pam Pettnot was excused from Executive Session.

Motion by Manager Rogers and seconded by Manager Shirley, the Board exit Executive Session at 7:17pm.

The motion was passed upon the following vote:

VOTE								
Salman Abbasey, MD	X	Yes		No		Abstain		Absent
Jerry Davis	X	Yes		No		Abstain		Absent
Bryan Kehl	X	Yes		No		Abstain		Absent
Rich Kosmerl	X	Yes		No		Abstain		Absent
Steve Perkins	X	Yes		No		Abstain		Absent
J. Thomas Reagan, MD	X	Yes		No		Abstain		Absent
Larry Rogers	X	Yes		No		Abstain		Absent
Janice Shirley	X	Yes		No		Abstain		Absent
James Wawrzyniak, DC	X	Yes		No		Abstain		Absent
VOTE TOTAL:	9	Yes	0	No	0	Abstain	0	Absent
RESULTS	**X**	**PASS**				**FAIL**		

EXECUTIVE SESSION DISCUSSIONS
President Kosmerl reminded attendees that all information discussed in executive session shall remain confidential and declared that no motions or votes were enacted on during the executive session.

NEXT REGULAR MEETING
The next regular meeting is scheduled for Tuesday, February 24, 2026 at 4:00pm.

ADJOURN
There being no further business to come before the Board, the meeting duly adjourned at 7:18pm upon motion by Manager Perkins.

James Wawrzyniak, DC, BOM Secretary Date

Pam Pettnot, Recording Secretary Date

WCCHS
Wyoming County Community Health System

Department Information Technology

POLICY: Written Information Security Policy (WISP)

PURPOSE: The purpose of the WISP is to better:

1) Ensure the security and confidentiality of **personally identifiable information (PII) and personal health information (PHI)** of customers, clients, employees, or vendors, as well as **sensitive company data,** which includes emails, confidential company information (i.e. company expansion plans, manufacturing processes, highly secretive information, etc.), employee information and the like.

2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information; and

3) Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft, fraud, or harm to WCCHS.

PROCEDURE:

Scope of Policy

In formulating and implementing the WISP, WCCHS has addressed and incorporated the following protocols:

1) Identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing PII and sensitive company data.

2) Assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the PII and sensitive company data.

3) Evaluated the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risk.

4) Designed and implemented a WISP that puts safeguards in place to minimize identified risks.

5) Implemented regular monitoring of the effectiveness of those safeguards.

Security Safeguards

The following safeguards are effective immediately. The goal of implementing these safeguards is to protect against risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing PII or sensitive company data.

Administrative Safeguards

1) **Chief Information Security Officer**- WCCHS has designated **the WCCHS Director of Healthcare Information Systems** to implement, supervise and maintain the WISP. This designated employee (the "Chief Information Security Officer") will be responsible for the following:

   (a) Implementation of the WISP including all provisions outlined in **Security Safeguards.**

   (b) Training of all employees that may have access to PII, PHI and sensitive company data. Employees should receive annual training, and new employees should be trained as part of the new employee hire process.

   (c) Regular monitoring of the WISP's safeguards and ensuring that employees are complying with the appropriate safeguards.

   (d) Evaluating the ability of any Third-Party Service Providers to implement and maintain appropriate security measures for the PII and sensitive company data to which WCCHS has permitted access, and requiring Third Party Service Providers, by contract, to implement and maintain appropriate security measures.

   (e) Reviewing all security measures at least annually, or whenever there is a material change in WCCHS's business practices that may put PII and sensitive company data at risk.

   (f) Investigating, reviewing, and responding to all security incidents or suspected security incidents.

2) **Security Management** - All security measures will be reviewed at least annually, or whenever there is a material change in WCCHS's business practices that may put PII or sensitive company data at risk. This should include performing a security risk assessment, documenting the results, and implementing recommendations of the security risk assessment to better protect PII and sensitive company data. The Chief Information Security Officer will be responsible for this review and will communicate to management the results of that review and any recommendations for improved security arising out of that review.

3) **Minimal Data Collection -** WCCHS will only collect PII of clients, customers, or employees that is necessary to accomplish legitimate business transactions or to comply with any and all federal, state, or local regulations.

4) **Information Access** - Access to records containing PII and/or sensitive company data shall be limited to those people whose job functions require a legitimate need to access the records. Access to the records will only be for a legitimate job-related purpose. In addition, pre-employment screening should take place to protect PII and sensitive company data.

5) **Employee Termination -** Terminated employees must return all records containing PII and sensitive company data, in any form, that may be in the former employee's possession (including all information stored on laptops or other portable devices or media, and in files, records, work papers, etc.). A terminated employee's physical and electronic access to PII and sensitive company data must be immediately blocked. A terminated employee shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to WCCHS's premises or information. A terminated employee's remote electronic access to PII and sensitive company data must be disabled; his/her voicemail access, e-mail access, internet access, and passwords must be invalidated.

6) **Security Training** – All employees, which includes all managers, employees, all independent contractors, and temporary employees that may have access to PII and sensitive company data, will receive security training. Employees should receive at least annual training, and new employees should be trained as part of the new employee hire process. Employees should be required to show their knowledge of the information and be required to pass an exam that demonstrates their knowledge. Documentation on employee training should be kept and reviewed.

7) **WISP Distribution -** A copy of the WISP is to be distributed to each current employee and to each new employee on the beginning date of their employment. It shall be the employee's responsibility to acknowledge in writing or electronically that he/she has received a copy of the WISP and will abide by its provisions. **See - Written Information Security Policy (WISP) Appendix A – WISP Employee Acknowledgement Form.**

8) **Contingency Planning** – All systems that store PII and/or sensitive company data should have the data backed upon, at least, a nightly basis. Data should be encrypted and stored offsite. Disaster Recovery mechanisms and documented procedures should be in place to restore access to PII and sensitive company data as well as any operating systems that WCCHS relies on. A system criticality assessment should be performed that defines how critical each of WCCHS's systems is. Systems that are critical to operations should be restored before non-critical systems. On a periodic basis, data backups, data restoration, and Disaster Recovery procedures should be tested and validated.

9) **Security Incident Procedures** - Employees are required to report suspicious or unauthorized use of PII and/or sensitive company data to a supervisor or the Chief Information Security Officer. Whenever there is an incident that requires notification pursuant to any federal or state regulations, the Chief Information Security Officer will conduct a mandatory post-incident review of the events and actions taken to determine how to alter security practices to better safeguard PII and sensitive data.

10) **Emergency Operations** – Procedures should be in place to define how WCCHS will respond to emergencies. Procedures should include employee contact information, critical vendor contact information, important vendor account information, as well as any emergency operating procedures.

11) **Data Sensitivity Classification** – All data that WCCHS stores or accesses should be categorized in terms of the sensitive nature of the information. For example, PII and sensitive company data might have a very high sensitivity and should be highly protected. Whereas publicly accessible information might have low sensitivity and requires minimal protection.

12) **Third Party Service Providers** - Any service provider or individual ("Third Party Service Provider") that receives, stores, maintains, processes, or otherwise is permitted access to any file containing PII and/or sensitive company data shall be required to protect PII and sensitive company data. The Third-Party Service Providers must sign service agreements that contractually hold them responsible for protecting WCCHS's data. Examples include third parties who provide off-site backup of electronic data; website hosting companies; credit card processing companies; paper record copying or storage providers; IT / Technology Support vendors; contractors or vendors working with customers and having authorized access to PII and/or sensitive company data.

13) **Sanctions** - All employment contracts, where applicable, should be amended to require all employees to comply with the provisions of the WISP and to prohibit any nonconforming use of PII and/or sensitive company data as defined by the WISP. Disciplinary actions will be taken for violations of security provisions of the WISP (The nature of the disciplinary measures may depend on several factors including the nature of the violation and the nature of the PII and/or sensitive company data affected by the violation).

14) **Bring Your Own Device (BYOD) Policy** – WCCHS may allow employees to utilize personally owned smartphones. If allowed, proper safeguards must be implemented to protect PII and sensitive company data that may be accessed or stored on these devices. Employees must understand what the requirements are for using personally owned devices and what safeguards are required.

Physical Safeguards

15) **Facility Access Controls** – WCCHS will implement physical safeguards to protect PII and sensitive company data. There will be physical security on facilities/office buildings to prevent unauthorized access. All systems that access or store PII and/or sensitive company data will be physically locked. Employees will be required to maintain a "clean desk" and ensure that PII and/or sensitive company data is properly secured when they are not at their desk. The Chief Information Security Officer will maintain a list of lock combinations, passcodes, keys, etc., and which employees have access to the facilities and PII and/or sensitive data. Visitors will be restricted from areas that contain PII and/or sensitive company data.

16) **Network Security** – WCCHS will implement security safeguards to protect PII and sensitive company data. Safeguards include; isolating systems that access or store PII and/or sensitive company data, the use of encryption on all portable devices, physical protection on portable devices, ensuring that all systems run up-to-date anti-malware, implementing network firewalls, performing periodic vulnerability scans, penetration testing, capturing and retaining network log files as well as ensuring that servers and critical network equipment are stored in an environmentally safe location.

Technical Safeguards

17) **Access Control** - Access to PII and sensitive company data shall be restricted to approved active users and active user accounts only. Employees will be assigned unique user accounts and passwords. Systems containing PII and sensitive company data should have automatic logoff procedures to prevent unauthorized access.

18) **Computer Use** – All employees will be given a Computer Use Policy that defines acceptable and unacceptable use of WCCHS's computing resources. Employees should be required to sign the Computer Use Policy to acknowledge acceptance of the policy.

19) **Data Disposal** - Written and electronic records containing PII and sensitive company data shall be securely destroyed or deleted at the earliest opportunity consistent with business needs or legal retention requirements.

20) **System Activity Review** - All systems that store or access PII and sensitive company data should utilize a mechanism to log and store system activity. Periodic system activity reviews should occur and identify unauthorized access to PII and sensitive company data. Any unauthorized access should be reported to the HIPAA Security Officer.

21) **Encryption** - To the extent technically feasible, all portable devices that contain PII and sensitive company data should be encrypted to protect the contents. In addition, encryption should be used when sending any PII and sensitive company data across public networks and wireless networks. Public networks include email and Internet access.

Appendix A – WISP Employee Acknowledgement Form

I have read, understand and agree to comply with the Written Information Security Policy (WISP), rules, and conditions governing the security of PII and sensitive company data. I am aware that violations of the WISP may subject me to disciplinary action and may include termination of my employment.

By signing this Agreement, I agree to comply with its terms and conditions. Failure to read this Agreement is not an excuse for violating it.

Signature	Date
Employee's Supervisor Signature	Date

REFERENCE(S):

Acceptable Use
Downtime and Contingency
Incident Response

Approver(s):	Click or tap here to enter text.
Review Date(s):	Click or tap to enter a date.
Effective Date:	Click or tap to enter a date.
Original Date:	Click or tap to enter a date.