☑OK To Use

AUDIT NAME
2024 Standard XII Health Information Systems

PASSING %
100

☐Consumer linked to this audit

☐ Staff Audit

SECTIONS

Section

NUMBERTITLE
1 XII. Administrative Safeguards - Security Management

SECTION QUESTIONS

Questions			
1	12.1 An individual has been recognized as a HIPAA Security or Privacy officer.	Met/Partially Met/Not Met	N/A
2	12.2 The CMHSP has developed and documented an appropriate Risk Assessment evaluation to ensure continuity of critical business processes.	Met/Partially Met/Not Met	N/A
3	12.3 Sanctions are in place for workforce members that fail to comply with security, acceptable use, or compliance policies and procedures.	Met/Partially Met/Not Met	N/A
4	12.4 Policies or procedures are in place for monitoring logs and audited activity of information systems.	Met/Partially Met/Not Met	N/A
5	12.5 An Incident Response plan is in place to address and respond to security incidents.	Met/Partially Met/Not Met	N/A
6	12.6 Breach identification and notification: Following the discovery of a breach of unsecured PHI, the CMHSP notifies all relevant parties within the required timeframes/timeline as required.	Met/Partially Met/Not Met	N/A
7	12.7 Breach notification content and delivery: The notification is written in plain language, and includes, to the extent possible:	Met/Partially Met/Not Met	N/A
8	12.7a A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.	Met/Partially Met/Not Met	N/A
9	12.7b A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved).	Met/Partially Met/Not Met	N/A

10	12.7c Any steps individuals should take to protect themselves from potential harm resulting from the breach.	Met/Partially Met/Not Met	N/A
11	12.7d A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches	Met/Partially Met/Not Met	N/A
12	12.7e Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.	Met/Partially Met/Not Met	N/A
13	12.7f The Written notification must be sent by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.	Met/Partially Met/Not Met	N/A
14	12.7g If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under §164.502(g)(4) of subpart E), written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available	Met/Partially Met/Not Met	N/A
15	12.8 Breach substitute notice: In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual under paragraph (d)(1)(i) of this section,	Met/Partially Met/Not Met	N/A
16	12.8a A substitute form of notice reasonably calculated to reach the individual shall be provided.	Met/Partially Met/Not Met	N/A
17	12.8b Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii).	Met/Partially Met/Not Met	N/A
18	12.8c In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided	Met/Partially Met/Not Met	N/A

	by an alternative form of written notice, telephone, or other means. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall:		
19	12.8c.1 Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside.	Met/Partially Met/Not Met	N/A
20	12.8c.2 Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.	Met/Partially Met/Not Met	N/A

SECTION QUESTIONS
Questions

NUMBERTITLE

2 XII. Administrative Safeguards - Workforce Management

SECTION QUESTIONS			
Questions			
1	12.9 Job descriptions, policies, or procedures are used to determine who has the authority to authorized access to PHI.	Met/Partially Met/Not Met	N/A
2	12.10 Policies or procedures are in place for determining acceptable use for remote access users.	Met/Partially Met/Not Met	N/A
3	12.11 Policies or procedures are in place to ensure existing access to PHI is monitored on a regular basis, and that access to PHI Is removed when no longer required for a job function.	Met/Partially Met/Not Met	N/A
4	12.12 Policies or procedures are in place for disabling employee access to PHI when an employee is terminated or leaves the agency.	Met/Partially Met/Not Met	N/A
5	12.13 The CMHSP has a process for identification of IT needs and assuring adequate IT resource allocation to fulfill contractually obligated functions.	Met/Partially Met/Not Met	N/A

SECTION QUESTIONS

Questions

NUMBERTITLE

3 XII. Administrative Safeguards - Security Awareness and Training

SECTION QUESTIONS			
Questions			
1	12.14 Workforce members are trained on the appropriate use of software systems, security, and their responsibility to protect PHI including appropriate use of Internet, email, and password management	Met/Partially Met/Not Met	N/A
2	12.15 Periodic security updates and trainings are conducted for workforce members.	Met/Partially Met/Not Met	N/A
3	12.16 A system is in place for workforce members to report technical issues and concerns, such as a help desk system.	Met/Partially Met/Not Met	N/A
4	12.17 The agency assures on-going learning for technical professionals to maintain currency in IT knowledge, skills, abilities, and certification.	Met/Partially Met/Not Met	N/A

SECTION QUESTIONS
Questions

NUMBERTITLE

4 XII. Administrative Safeguards - Contingency Planning

SECTION QUESTIONS			
Questions			
1	12.18 Data is backed up regularly, and restore process is tested periodically to ensure validity and usability of the backup media and restore procedures.	Met/Partially Met/Not Met	N/A
2	12.19 The CMHSP has a Disaster Recovery Plan.	Met/Partially Met/Not Met	N/A
3	12.20 The Disaster Recovery Plan is tested regularly, and the process is documented.	Met/Partially Met/Not Met	N/A
4	12.21 Data is archived, and policies or procedures detail that data is kept or archived for a minimum of 6 years.	Met/Partially Met/Not Met	N/A
5	12.22 The CMHSP has an Emergency Mode Plan for operating only critical business processes during an incident, disaster, or natural event.	Met/Partially Met/Not Met	N/A

SECTION QUESTIONS
Questions

NUMBERTITLE

5 XII. Administrative Safeguards - Compliance Assurance

SECTION QUESTIONS			
Questions			
1	12.23 The CMHSP uses Business Associate Contracts and Data Use Agreements when sharing PHI with any and all outside vendors and organizations.	Met/Partially Met/Not Met	N/A
2	12.24 The CMHSP has policies or procedures in place for how to adhere to compliance requirements including HIPAA and handling PHI.	Met/Partially Met/Not Met	N/A
3	12.25 The CMHSP has had a 3rd party security audit conducted within 18 months, or has an audit scheduled within the next 6 months.	Met/Partially Met/Not Met	N/A

SECTION QUESTIONS
Questions

NUMBERTITLE

6 XII. Technical Safeguards - Access/Audit Controls

SECTION QUESTIONS			
Questions			
1	12.26 Unique user IDs are assigned to all users.	Met/Partially Met/Not Met	N/A
2	12.27 A system is in place to maintain access controls and authentication mechanism (ex. Active Directory).	Met/Partially Met/Not Met	N/A
3	12.28 Access controls to PHI are managed using the concept of “least privilege” and changes are made by approved administrative staff only.	Met/Partially Met/Not Met	N/A
4	12.29 Emergency access policies or procedures are in place for accessing PHI in emergency situations.	Met/Partially Met/Not Met	N/A
5	12.30 Workstations are automatically logged off from or locked when unattended.	Met/Partially Met/Not Met	N/A
6	12.31 The CMHSP has methods for auditing logins, files, and PHI access.	Met/Partially Met/Not Met	N/A

SECTION QUESTIONS
Questions

NUMBERTITLE

7 XII. Technical Safeguards - Encryption and Integrity

SECTION QUESTIONS			
Questions			
1	12.32 PHI is encrypted when transmitted over a public electronic network. (ex. email, Internet, VPN).	Met/Partially Met/Not Met	N/A

2	12.33 The CMHSP uses email encryption when sending PHI via email.	Met/Partially Met/Not Met	N/A
3	12.34 End user devices (PCs, laptops, phones) storing PHI are encrypted.	Met/Partially Met/Not Met	N/A
4	12.35 Systems storing PHI are encrypted or have reasonable physical security limiting direct physical access to PHI to authorized individuals only.	Met/Partially Met/Not Met	N/A
5	12.36 A mobile device management system is used to enforce security, access control, compliance and encryption rules to mobile devices accessing PHI.	Met/Partially Met/Not Met	N/A
6	12.37 The CMHSP uses modern encryption standards for encrypting removable media containing PHI. (flashdrives, memory cards, CD/DVDs, disks, etc.)	Met/Partially Met/Not Met	N/A
7	12.38 The CMHSP uses modern authentication and encryption technologies to encrypt agency wireless network traffic. (ex. WPA, WPA2, TKIP, AES).	Met/Partially Met/Not Met	N/A

SECTION QUESTIONS
Questions

NUMBERTITLE

8 XII. Technical Safeguards - Workstation Security

SECTION QUESTIONS			
Questions			
1	12.39 Operating systems used are currently supported, and not out of date.	Met/Partially Met/Not Met	N/A
2	12.40 Operating system and software updates are applied to systems on a regular scheduled basis.	Met/Partially Met/Not Met	N/A
3	12.41 Endpoint security software/ antivirus is installed on all devices.	Met/Partially Met/Not Met	N/A
4	12.42 The CMHSP uses secure remote access software or a VPN to access systems containing PHI remotely.	Met/Partially Met/Not Met	N/A

SECTION QUESTIONS
Questions

NUMBERTITLE

9 XII. Physical Safeguards - Facility Controls

SECTION QUESTIONS

Questions			
1	12.43 The CMHSP has a method for tracking access to a facility with PHI for authorized users and visitors. (ex. keycards, receptionist)	Met/Partially Met/Not Met	N/A
2	12.44 The CMHSP maintains an organizational chart.	Met/Partially Met/Not Met	N/A
3	12.45 The CMHSP maintains a network diagram including an overview of the current network topology.	Met/Partially Met/Not Met	N/A
4	12.46 The CMHSP maintains an updated hardware inventory including location and/or who is responsible for each hardware item.	Met/Partially Met/Not Met	N/A

SECTION QUESTIONS
Questions

NUMBERTITLE

10 XII. Physical Safeguards - Workstation, Device, and System Security

SECTION QUESTIONS			
Questions			
1	12.47 The CMSHP has workstation use policies or procedures in place for devices accessing PHI.	Met/Partially Met/Not Met	N/A
2	12.48 The CMSHP has acceptable use policies or procedures in place for users accessing PHI.	Met/Partially Met/Not Met	N/A
3	12.49 The CMHSP manages a firewall and uses VLANs to prevent unauthorized remote access to systems.	Met/Partially Met/Not Met	N/A
4	12.50 Physical security measures are in place to restrict access to non-user IT resources. (ex. servers, network equipment, datacenters	Met/Partially Met/Not Met	N/A
5	12.51 A password policy is in place for authenticating access to system resources containing PHI.	Met/Partially Met/Not Met	N/A
6	12.52 Policies and procedures are in place for IT resource acquisition including new hardware and licensing.	Met/Partially Met/Not Met	N/A
7	12.53 The CMHSP has a refresh cycle in place for replacing obsolete and depreciated IT resources.	Met/Partially Met/Not Met	N/A
8	12.54 The CMHSP has a policy or procedure in place for disposing of electronic devices and media that contain PHI. (PCs, laptops, disks, memory cards, flash drives, etc.)	Met/Partially Met/Not Met	N/A

SECTION QUESTIONS			
Questions			

NUMBERTITLE
11 XII. Contractual Obligations

SECTION QUESTIONS			
Questions			
1	12.55 The CMHSP combines different types of information to provide complex required data feeds to the PIHP including BH-TEDS, QI, claims/ encounters, critical incidents, and performance indicator data.	Met/Partially Met/Not Met	N/A
2	12.56 The CMHSP submits encounters to LRE monthly in accordance with the CMHSP's responsibilities outlined in the LRE/CMHSP delegation grid.	Met/Partially Met/Not Met	N/A
3	12.57 The CMHSP submits refreshed Consumer List data to LRE on a regular basis, weekly at minimum.	Met/Partially Met/Not Met	N/A
4	12.58 The CMHSP submits BH-TEDS files and QI files to LRE monthly in accordance with the CMHSP's responsibilities outlined in the LRE/CMHSP delegation grid.	Met/Partially Met/Not Met	N/A
5	12.59 The CMHSP participates in Health Information Exchanges (HIE) within the region as allowed by state and federal laws and regulations.	Met/Partially Met/Not Met	N/A
6	12.60 The CMHSP uses information at its disposal to ensure adequate and appropriate engagement of delegated functions.	Met/Partially Met/Not Met	N/A
7	12.61 The CMHSP submits provider data to the PIHP no less often than once every 28 days [every 14 days recommended] that includes complete and properly formatted data which meets all Provider Directory requirements as by defined contract and by federal regulations including the MDHHS/ PIHP contract, LRE P6.3.1. PIHP Customer Services Standards, Medicaid Care Regulations-2016 Final Rule Update, and the 42 CFR 438.10 as defined in the LRE Provider Directory Policy (6.5).	Met/Partially Met/Not Met	N/A
8	12.62 The CMHSP uses the recommended best practice of linking their CMHSP website directly to the LRE (MI Recovery) online provider directory to provide consumers with access to the most updated and	Met/Partially Met/Not Met	N/A

	accurate provider information in a searchable and filterable interface.		
9	12.63 The CMHSP has general system controls and quality procedures in place to verify the validity and reliability of data submissions transmitted to the PIHP. Additionally, the CMHSP has policies or specific work procedures in place associated with each individual data submission type, to guide the appropriate validation, submission, and reconciliation processes for each, ensuring data completeness and reliability for BH-TEDS, QI, claims/ encounters, critical incidents, and performance indicator data.	Met/Partially Met/Not Met	N/A

SECTION QUESTIONS
Questions

SECTIONS
Section