1044 Gibert St.
Flint, MI 48532
(810)422-9406
(810)733-7623 fax

31581 Gratiot Ave
Roseville, MI 48066
(586)783-4802
(586)783-4805 fax

Risk Analysis/Plan
FY 2024-2026

BioMed Behavioral Health Services (updated 12/2024)

ELECTRONIC PROTECTED HEALTH INFORMATION

RISK ANALYSIS PER 45 CFR §164.308(8)

DATE OF REVIEW: August 07, 2024

I. INTRODUCTION

This is an audit conducted under 45 CFR §164.308 to assess risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) of patients who have applied for, are receiving, or who have received treatment at BIOMED.

II. RISK MANAGEMENT

Risk for unauthorized access to ePHI remains low, due to established structure requiring username/passwords at each layer (PC Station, Private Network, Google Workspace and SMART) before ePHI can be accessed. Additional factors contributing to low risk for unauthorized access to ePHI are addressed below.

III. CONFIDENTIALITY

All ePHI is kept on an encrypted electronic medical record platform (SMART) provided by Smart Management, Inc., Providence, Rhode Island. SMART is certified by claredi.com as a HIPAA compliant software platform.

Biomed utilizes HIPAA Vault through Google Workspace for securely hosting and construction of its website and employee's company email accounts. HIPAA Vault provides HIPAA Compliant Cloud Solutions to healthcare organizations to protect Patient Health Information (PHI) data under the HIPAA and HITECH Act and carries the following certifications, NAICS 518210, SBA8a 306508, CAGE 6KKB2, DUNS 847209848, CA DBE 42400, CA SBE 6699. Through HIPAA Vault our website and email data stored in the cloud is encrypted with AES-256 symmetric cryptography and your data in transit is encrypted with an RSA 2048 bit key.

IV. INTEGRITY

In order to protect the integrity of ePHI, users must first login to each PC station using an assigned username and password. Thereafter, users must login to a secure cloud facility that provides access to ePHI using an assigned username and password, changed bi-annually by Smart management.

1044 Gibert St.
Flint, MI 48532
(810)422-9406
(810)733-7623 fax

31581 Gratiot Ave
Roseville, MI 48066
(586)783-4802
(586)783-4805 fax

V. AVAILABILITY

Access to ePHI is provided via a secure and encrypted connection to the SMART ePHI platform, which is located on a secure private virtual server accessible only via PC stations within our network, access to which is restricted to the public IP address of our clinic.

VI. SANCTION POLICY

Improper use of ePHI is a violation of the Codes of Ethics formulated by the National Association of Social Workers, National Board of Certified Counselors, the International Credentialing & Reciprocity Consortium, the Michigan Certification Board for Addiction Professionals, and BioMed Behavioral Health Services . Disciplinary measures for ethics violations include, but are not limited to, written reprimand with required remedial training, suspension without pay, termination, and violation reporting to the applicable licensing and certification boards.

VII. INFORMATION SYSTEM ACTIVITY REVIEW

Audit log reports, access reports, and security incident reports related to ePHI are monitored on a daily basis by Smart Management. Audit log reports, access reports, and security incident reports related to non ePHI ,i.e. local, network infrastructure are monitored daily by Megatechnologies, which neither has access to nor credentials for the ePHI system. Significant deviations from the norm, such as an incidence of login failure that exceeds what would be expected from typing errors are investigated and brought to management’s attention.

VIII. ASSIGNED SECURITY RESPONSIBILITY

BIOMED's Corporate Compliance Officer is responsible for the development of policies and procedures to prevent improper use and unauthorized access to ePHI. BIOMED's Corporate Information Technology Manager is responsible for their implementation

IX. WORKFORCE SECURITY

All members of the treatment team including, front desk personnel, office managers, medical assistants, admission coordinators, billing staff, medical staff, nursing staff, clinical supervision, clinical counseling staff, and executive management personnel are provided with appropriate privileges to access ePHI, as appropriate to their respective functions.

Executive management personnel are provided with high-level administrative privileges that include the privileging of new staff and termination of ePHI access privileges for terminated staff.

Medical Staff/Nursing Staff (Medical assistants) are provided with mid-level administrative privileges, which allow staff in this category to enter and access ePHI, such as medication orders, prescriptions, nursing assessment, and other related medical progress notes, such as urine drug screen results, Hepatitis C blood screen results, and Tuberculosis screen results.

Admission coordinators are provided with low-level administrative privileges, which allow staff in this category to enter and access new patient ePHI for initial assessment by clinical, medical, and nursing staff.

Clinical supervision staff are provided with low-level administrative privileges, which allow

1044 Gibert St.
Flint, MI 48532
(810)422-9406
(810)733-7623 fax

31581 Gratiot Ave
Roseville, MI 48066
(586)783-4802
(586)783-4805 fax

staff in this category access to ePHI to assign and transfer patients to the various clinical counselors on staff and countersign treatment plans, assessments, and requests for off-site dosing privileges.

Clinical counseling staff are provided with clinical privileges, which allow staff in this category to enter and access ePHI, such as releases of information, consents for treatment, progress notes, treatment plans, assessments, and requests for off-site dosing privileges.

Front desk personnel (Office managers) are provided with clerical privileges, which allow staff in this category to access ePHI to check-in patients, triage and route patients to appropriate providers, track attendance, and review financial information for payment processing.

Billing staff are provided with billing privileges, which allow staff in this category to access ePHI to review services provided and reconcile with applicable funding source information for billing purposes.

Building and grounds maintenance personnel are not permitted to access ePHI and are not given username/password access to PC Stations in the first instance.

X. AUTHORIZATION AND/OR SUPERVISION

Daily supervision of workforce members authorized to access ePHI is provided by the head of each department, or designated supervising team leader.

XI. WORKFORCE CLEARANCE PROCEDURE

All staff requiring ePHI access are required to undergo a criminal background check, a Centers for Medicaid and Medicare Services/Office of Inspector General exclusion check, and credential, licensure, and degree verification, as applicable.

Qualified staff are assigned to a PC station and are provided access with appropriate administrative, billing, clerical, clinical, or medical privileges (See Section IX) for SMART ePHI functions.

The Corporate Information Technology Manager configures New PC stations/equipment and assigns a username and password for each new user. Thereafter, each staff member is provided with login privileges to the private network and username and password for SMART ePHI platform.

XII. TERMINATION PROCEDURES

Upon termination of a staff member with ePHI access, notification is sent to Corporate Information Technology Manager) for immediate deactivation.

XIII. SECURITY AWARENESS AND TRAINING

All staff are trained in the Code of Ethics established by the Michigan Certification Board for Addiction Professionals, which includes training on the confidentiality requirements under HIPAA and 42 CFR Part II. Staff are trained in the importance of using measures to safeguard ePHI, such as using privacy screens for PC monitors in high-traffic areas and locking individual office doors while

1044 Gibert St.
Flint, MI 48532
(810)422-9406
(810)733-7623 fax

31581 Gratiot Ave
Roseville, MI 48066
(586)783-4802
(586)783-4805 fax

temporarily away from their offices to prevent inadvertent or surreptitious access to ePHI.

XIV. PERIODIC SECURITY UPDATES

Smart, Management . and Megatechnologies Inc conduct ongoing security updates to its SMART ePHI platform and local network facilities respectively outside of BIOMED's hours of operation.

XV. PROTECTION FROM MALICIOUS SOFTWARE

In order to increase protection of ePHI against malware and viruses, internet access is restricted to sites required for specific work purposes only. Staff may submit a request for access to a site for a particular purpose, such as professional development, community resources, etc, which must be approved by the Corporate Information Technology Manager. Additionally all internet access is managed by a CISCO security device which also scans for issues. Also each PC workstation has installed a malicious software protection application.

XVI. LOG-IN MONITORING

. Daily alerts inform Corporate Information Technology Manager of inconsistencies in login attempts. Daily reports of all successful and unsuccessful login attempts to access SMART ePHI, Google Workspace, and local network infrastructure platforms are also available through SMART Management, Google Workspace, and Megatechnologies respectively.

XVII. PASSWORD MANAGEMENT

Passwords for access to each PC station are set/reset by the Corporate Information Technology Manager only. Access to each PC station remains blocked, unless the correct password is entered. Station screens lock after 5 minutes of inactivity and require a password to regain access.

Passwords for access to the private network are set/reset by the Corporate Information Technology Manager only. Access to the private network remains blocked, unless the correct password is entered.

Passwords for SMART ePHI platform are known to the user only. Passwords for SMART ePHI are required to be reset every 6 months. Security questions with answers known to the user only must be correctly answered for password reset.

XVIII. SECURITY INCIDENT PROCEDURES—RESPONSE & REPORTING

In the event ePHI is believed to have been compromised, the Corporate Compliance Officer receives immediate notification and initiates a prompt incident investigation. The Officer establishes a special committee to investigate incidents and determine if the incident rises to the level of a breach. The committee presents its findings, which may include, but are not limited to, the harmful effects of such breach to BIOMED, recommendations for mitigation of breach, and recommendations for improved security measures. The results of incident investigations, breach notification, and training records are maintained for at least ten years.

1044 Gibert St.
Flint, MI 48532
(810)422-9406
(810)733-7623 fax

31581 Gratiot Ave
Roseville, MI 48066
(586)783-4802
(586)783-4805 fax

XIX. DATA RETENTION & RECOVERY—EMERGENCY PREPAREDNESS

All ePHI is backed up on a HITECH compliant, secure, off-site server on a continuous basis by SMART Management. SMART's PHI database is constantly backed up every 5-7 minutes using the AWS Aurora MySQL database platform. Additionally, the database and file system are backed up daily and archived for a minimum period of seven years. They are stored to AWS S3All saved ePHI is recoverable in the event of a disaster resulting in the loss of ePHI.

An up-to-date patient list with relevant medical data printed daily is available in the event of a loss of power, catastrophic event, or other circumstance which results in the inoperability of PC stations necessary for access to ePHI. This list is utilized to administer medication to patients when ePHI is unavailable.

In the event of a catastrophic event or other circumstance which results in the destruction of property that prevents recovery of ePHI or printed patient data, the Medical Director or Executive Director is authorized to access and retrieve ePHI stored on a secure, off-site server for continued business operations at a temporary site.

XX. REMOTE ACCESS

Due to the challenges of Covid-19, BIOMED has deemed it necessary to provide remote access to our ePHI while working at home. BIOMED has elected to utilize Remote access via Barracuda Networks . This program provides an encrypted connection to the PC that employees already have assigned to them on site. Only users authorized by the management team are eligible for remote access via this system from home. This program enables BIOMED to utilize all of the security protocols it already has in place for ePHI.

The access through Barracuda Networks is monitored by Megatechnologies Inc., which promptly deletes accounts of staff when notified by site management to do so.

XXI. RECOMMENDATIONS

1. While each PC Station is password-protected with an administrative password, potential risk for security breaches resulting in unauthorized access to ePHI can be further reduced by providing each staff member with his or her own password. Individual staff member passwords will also help to track any unsuccessful attempts to breach the first layer of security at the PC station.

2. While PC Stations in the reception area, nursing station, and other high-traffic areas are covered with privacy screens, potential risk for security breaches resulting in unauthorized access to ePHI can be further reduced by covering PC screens in private individual offices.

3. While staff is well-practiced in locking individual office doors while temporarily away from their offices to prevent inadvertent or surreptitious access to ePHI, potential risk for security breaches can be further reduced by reducing automatic time-out/log-off setting to 5 minutes.

1044 Gibert St.
Flint, MI 48532
(810)422-9406
(810)733-7623 fax

31581 Gratiot Ave
Roseville, MI 48066
(586)783-4802
(586)783-4805 fax

4. Biomed will be implementing Coded ID Badges that will facilitate access to each employee local PC and physical access to Biomed

5. www.biomedmat.org is the new website for Biomed. Over the past few months, Biomed has put together a mobile, computer, and tablet-friendly site. It has information for current and new patients about what we offer at both sites, office hours, and contact information. Biomed is working on adding more in-depth information about the services provided at each location, what to expect during your first visit, and other social services available in Macomb County and Region 10 PIHP. Updates and future plans for the web site are ongoing and include adding calendars that will update in real time for both the Flint and Roseville locations for events, group meetings, closures, and opportunities for patients. Biomed has been getting information from staff, patients and other community members about what they think will be helpful to everyone to have on the site and even working on our blog.

Created 8/2024; Reviewed 12/2024