Compliance Newsletter

ISSUE 1 / JUNE 2024 SWMBH OPERATING POLICY: 10.18

BREACH NOTIFICATION

- A breach occurs when there is an unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of that information.
- If you suspect or know of any situation involving a potential breach, it is your responsibility to report it to the Compliance Department.
- Breach reports are reviewed monthly by the breach team. Pending results, a decision is made as to if the breach is reportable. Depending on the severity, notification may occur to the customer, media or Office of Civil Rights.

NEW BREACH REPORTING METHOD

The compliance team is excited to announce the official rollout of our new breach reporting system using SmartSuite. We encourage you to use it and share any feedback with us to help improve its effectiveness and user-friendliness.

Link for reporting:
https://form.smartsuite.com/ssn4yl4x/RGbCvWAwnU

EMAIL TO THE WRONG PERSON

The number one reported breach in fiscal year 2023. If you email PHI to the wrong individual, reach out and ask them to double delete the email. This can be avoided by occasionally clearing email auto fill and double checking the recipient.

UNENCRYPTED EMAIL & PHI IN SUBJECT LINE

The second most reported breach. Be aware that subject lines are NOT encrypted. Best practice is to keep those subject lines free of PHI. Also keep 'ecrypt' in your subject line OR body of the email. You can keep 'ecrypt' in your signature to avoid forgetting to add this.

PHI SHARED ON TOOLS SENT TO PROVIDERS

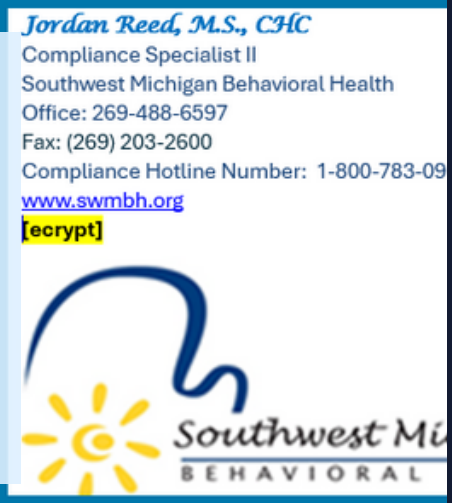
The third most frequent reported breach is sending out emails with tools for providers that still have PHI attached. Please double check that all fields are blank before hitting send. Ask for the email to be double deleted if sent out.

Compliance Newsletter

Issue 1 / June 2024

SWMBH Operating Policy: 10.18

Best way to keep emails encrypted



A NOTE FROM IT ON ENCRYPTION CHANGES

We're upgrading our email encryption platform! On Sunday, June 9th, we'll be replacing Zix Email Encryption with Microsoft's platform. Going forward, encrypted emails from SWMBH will now be delivered via Microsoft encryption, removing the requirement to log into the Zix portal. Recipients can automatically access encrypted emails from SWMBH directly in their Outlook email clients. For non-Outlook users, Microsoft Authentication services will guide them. Have questions? Reach out to the IT team.

MEET THE BREACH TEAM!

Your breach team meets and discusses the reports monthly! This team is made up of five individuals.

- **Mila Todd**: Cheif Compliance Officer and Provider Network Director
- **Alison Strasser**: Compliance Specialist
- **Beth Guisinger**: Director of Utilization Management
- **Natalie Spivak**: Chief Information Officer
- **Garyl Guidry**: Chief Financial Officer