SECURITY & DATA BREACH NOTIFICATION GUIDANCE FOR COMMUNICARE NETWORK PARTNERS
Effective Date: March 1, 2024

Wyoming 211, through CommuniCare, is excited to work with CommuniCare Network Partners to improve the lives of the residents in our state. We are also committed to protecting the privacy and security of individuals' information.

As the backbone agency supporting CommuniCare, we aim to ensure that system users do not intend to collect and share data that could be unintentionally or intentionally used against any population, especially individuals, through creating or emphasizing bias or other harmful polarizing narratives. Wyoming 211 will follow the requirements of the HIPAA Breach Notification Rule for PHI breaches and we will also follow the Wyoming Breach Notification Statute for any PII breaches.

This document provides guidance for Partner Agencies on Risk Reduction Efforts, Software and Hardware Recommendations, and to know how to identify a potential breach, investigate that breach and notify appropriate agencies.

Risk Reduction Efforts:
Communicare meets rigorous security standards to protect client PHI from being shared with unauthorized users. HIPAA requires a regular internal Security Risk Assessment. Wyoming 211 IT staff will also conduct a regularly scheduled vulnerability scan and update risk observations to help prioritize cybersecurity and IT efforts.

Visionlink, Communicare's technology platform vendor, uses an unbiased third party, Amazon Web Services, to certify its security status. The work to meet HIPAA requirements requires third-party auditors (Amazon Web Services), risk analysis and remediation, vulnerability scans and penetration testing, and protected virtual workspaces through which Visionlink staff manages Wyoming 211's/Communicare Visionlink systems. To protect HIPAA compliant data, Visionlink has deployed separate instances of Amazon Web Services for Communicare and Wyoming 211.

Software and Hardware Recommendations:
Software:

1. The Visionlink CRM is supported by any browser, however the following are recommended:
    a. Google Chrome (recommended – latest version)
    b. Mozilla Firefox (recommended – latest version)
2. For all points of entry to the system use supported and updated to Operating System Manufacturer specifications.
3. Apply all current security patches and updates for Operating Systems and Applications
4. Use business-grade Anti-Virus software and keep it up to date.
5. The use of encryption is strongly recommended.
6. Securely archive any encryption keys.
7. Use a password manager and ensure passwords are long (greater than 12 characters) and strong (using a combination of uppercase, lowercase, numbers and special characters).
8. Enable Multifactor Authentication (MFA) for your device, applications and any websites you access.
9. Do not re-use passwords across logins.

10. Each user must have their own login to the software (Visionlink) and all passwords must be protected. Sharing log in information is strictly forbidden.

Hardware:

1. Accessing the Visionlink CRM must be on a private network connection
2. Hardware that is accessing Visionlink CRM must have password protection and auto-locking capabilities and passwords may not be shared.

DEFINITIONS

Personal Identifying Information (PII) is any information that can be used to distinguish or trace an individual's identity.

1. Names
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Phone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers.
11. Certificate/license numbers.
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data)

Protected health information (PHI) is any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment. PHI includes the above examples as well as the following:

1. Medical diagnosis
2. Case management notes
3. Medication lists
4. Behavioral health/mental health records
5. Substance Use Disorder information

BREACH NOTIFICATION

In the event of any suspected breach of information, please notify admin@wyoming211.org immediately. If you believe that you are a victim of cybercrime, you may also notify your Internet Service Provider (ISP), local law enforcement agency (911) or to the Federal Bureau of Investigation (FBI) at https://www.ic3.gov/Home/FileComplaint. notify the authorities by dialing 911. The following guidance is designed to help you in determining what to do if you suspect a breach impacting CommuniCare information.

A Breach is defined as:

1. Reasonable belief that unencrypted personal information was acquired, or reasonably believed to have been acquired, by an unauthorized person; or in the case of encrypted personal information, it is reasonably believed that the encryption key or security credential was acquired by an unauthorized person and could render the healthcare or personal information readable.
2. A breach is generally an impermissible use or disclosure that compromises the security or privacy of the protected health information under the Privacy Rule *(Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 164, Subpart E)*. An impermissible use or disclosure of protected health information or personally identifiable information is presumed to be a breach unless the agency that maintains or transmits computerized data, demonstrates that there is a low probability that the protected health information or personally identifiable information has been compromised based on risk assessment.

Upon Learning of a Breach

A breach or a suspected breach of 211 data or systems, you must notify 211 at admin@wyoming211.org immediately. The following information must be reported:

- A description of how the breach happened.
- When the breach happened, including date and time of the breach and date and time of the discovery of the breach, if known.
- A description of the types of unsecured protected health information or personally identifiable 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, and how many individuals were affected?
- A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
- Contact procedures for individuals involved in the investigation.

In addition to this guidance, you are responsible for understanding your legal requirements for reporting directly to state and federal agencies.

For Protected Health Information (PHI) security and breach requirements or to understand your rights under HIPAA, refer to United States Department of Health and Human Services HIPAA website: https://www.hhs.gov/hipaa

Investigation of a Breach

211 management will make a record of events and people involved, as well as any discoveries made over the course of the investigation and determine whether or not a breach has occurred.

Perform a Risk Assessment

Once a breach has been verified and contained, perform a risk assessment that rates the following:

1. Sensitivity of the PII lost (customer contact information alone may present much less of a threat than financial information)
2. Amount of PII lost and number of individuals affected
3. Likelihood PII is usable or may cause harm
4. Likelihood the PII was intentionally targeted (increases chance for fraudulent use)
5. Strength and effectiveness of security technologies protecting PII (e.g., encrypted PII on a stolen laptop. Technically stolen PII but with a greatly decreased chance of access).
6. Ability of Wyoming 211 Inc. to mitigate the risk of harm

All information collected during the risk assessment must then be compiled into one report and analyzed. The risk assessment must then be provided to appropriate Wyoming 211 personnel in charge of data breach response management.

Notifying Affected Parties

Responsibility to notify is based both on the number of individuals affected and the nature of the PII/PHI that was accessed. Any information found in the initial risk assessment will be turned over to the legal counsel of Wyoming 211 who will review the situation to determine if, and to what extent, notification is required.

Notification should occur in a manner that ensures the affected individuals will receive actual notice of the incident. Notification will be made in a timely manner, but not so soon to unnecessarily compound the initial incident with incomplete facts or to make identity theft more likely through the notice.

In the case that notification must be made under these conditions:

1. Only those that are legally required to be notified will be informed of the breach. Notifying a broad base when it is not required could cause raise unnecessary concern in those who have not been affected.
2. A physical copy will always be mailed to the affected parties no matter what other notification methods are used (e.g., phone or email).
3. A help line will be established as a resource for those who have additional questions about how the breach with affect them.
4. The notification letter will include the following:
5. A brief description of the incident. The nature of the breach and the approximate date it occurred.
6. A description of the type(s) of PII that were involved in the breach (general types of PII, not an individual's specific information).
7. Explanation of what Wyoming 211 Inc. is doing to investigate the breach, mitigate its negative effects and prevent future incidences.
8. Steps the individual can take to mitigate any potential side effects from the breach.
9. Contact information for a Wyoming 211 Inc. representative who can answer additional questions.

Mitigating Risks

Based off the findings of the risk assessment, a plan will be developed to further mitigate risk involved with the breach. The exact course of action will be based on the type of PII/PHI that was involved in the data breach. The course of action will aim to minimize the effect of the initial breach and to prevent similar breaches from taking place.

Affected individuals will be notified as soon as possible so they can take their own steps to mitigate potential risk.

Wyoming 211 will also provide steps to mitigate risks that can be taken by affected individuals. The steps provided to affected individuals will depend on the nature of the data breach. If the breach has created a high risk for fraudulent use of financial information, customers may be advised to do the following:

1. Monitor their financial accounts and immediately report any suspicious or fraudulent activity.
2. Contact the three major credit bureaus and place an initial fraud alert on their credit reports. This can be extremely helpful in situations where PII that can be used to open new accounts, such as social security numbers, has been taken.
3. Avoid attempts from criminals that may see the breach as an opportunity to pose as Wyoming 211 Inc. employees in an attempt to deceive affected individuals into divulging personal information.
4. File a report with local police or in the community where the breach took place.
5. Complete a Federal Trade Commission Threat Affidavit, available at www.ftc.gov/opa/2002/02/idtheft.shtm. This form will allow the affected individual to notify their creditors that their identity has been compromised and will minimize their liability for fraudulent use of their identity.

Instructions on what steps a customer can take to reduce their risk will be included in the notification letter. In addition to the information listed above, appropriate Wyoming 211 personnel, when possible, will provide additional information tailored to the individual breach.

Thank you for your help in protecting the personal information of the individuals we serve.

Please feel free to contact 211 privacy and security team with any questions: admin@wyoming211.org.