

2-1-1 is excited to work with you to better the lives of residents in our community. 2-1-1 extends that commitment to the community by protecting the privacy and security of individuals' information. This provides guidance for Partner Agencies on software and hardware and to know how to identify a potential breach, investigate that breach and notify appropriate agencies.

Software and Hardware:

Software:

1. In order to use the Salesforce CRM, the following link provides a list of supported browsers:
https://help.salesforce.com/articleView?id=getstart_browser_overview.htm&type=0
2. All points of entry to the system should be supported and updated to Operating System Manufacturer specifications.
3. Anti-Virus software should be installed and kept current.
4. 2-1-1 strongly recommends the use of encryption when data is stored or transmitted over the internet.
5. Each user must have their own log-in to the software (Salesforce) and all passwords must be protected. Sharing log on information is strictly forbidden.

Hardware:

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

Breach Notification:

In the event of any suspected breach of information, please immediately notify privacy@211sandiego.org . If you believe you are the victim of cyber crime, you may also notify the authorities by dialing 9-1-1 or at www.catchteam.org. The following guidance is designed to help you in determining what to do if you suspect a breach impacting 2-1-1 information.

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

Definition of a Breach

- 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 or of personally identifiable information under California's Information Practices Act. 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 a risk assessment.
- 3)

What to do if you suspect a breach of 2-1-1 data or systems:

Immediately notify 2-1-1 at privacy@211sandiego.org

Include the following information in your e-mail:

- A brief description of what happened, including the date of the breach and the date 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).
- 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.

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>

For guidelines on protecting private information including Personally Identifiable Information (PII), see the California State Attorney General's guidelines on Cybersecurity:

<https://oag.ca.gov/cybersecurity>

If you believe you have been a victim of a cyber-crime, contact San Diego's Computer and Technology Crime High-Tech Response Team (CATCH) at:

<http://www.catchteam.org/>

To understand your breach reporting requirements under California Information Practices Act, See, [California Civil Code Section 1798-1798.78](#).

Client Consent:

Purpose is to ensure:

- Informed consent and authorization is obtained
- Same protocol is followed for each consented client

Consents and Authorizations:

Types of Consent:

- Wet Signature (See Appendix 1)
- Adobe Sign (See Appendix 1)
- Telephonic Signature (See Appendix 2)
- Text Message (See Appendix 3)

Types of Authorization:

- Wet Signature (See Appendix 4)
- Adobe Sign (See Appendix 4)

Definitions:

Consent: Consent embodies the concept that the Client is *informed* about the uses and disclosures that will be made of the information (as set forth in the Covered Entity’s Notice of Privacy Practices), the Client has legal capacity to make the decision and the decision to consent or refuse consent is made voluntarily.

Authorization: An Authorization refers to a type of formal consent to disclose healthcare information the form and contents of which must comply with state and federal laws in order to be valid. An Authorization must be in writing, 14pt font, signed and dated by the Client and must state what information the Client agrees will be disclosed, who the information may be disclosed to and the purpose of the disclosure. An Authorization must also include information advising the Client of their right to revoke, to obtain a copy, whether a healthcare provider can condition treatment, payment or eligibility on receipt of the authorization and that the information may not longer be protected if the recipient re-discloses the information. As a general rule, an Authorization is or may be required for the use and disclosure of “sensitive” healthcare information such as drug or alcohol abuse, HIV Test results, and psychotherapy notes. An Authorization is also required when a Covered Entity discloses healthcare information to a non-Covered Entity such as Meals on Wheels, uses healthcare information for certain marketing purposes and or sells PHI. When a patient’s authorization is required, voluntary consent is not sufficient.

Guidelines:

1. Agency Staff must ensure the client is sound body and mind, by asking the questions such as, “do you understand...”
2. Agency Staff must ensure the client can read/understand English or Spanish, by confirming the client speaks or read English or Spanish
3. Identify which type of consent or authorization client is needed. If PHI will be disclosed to 2-1-1 or a Partner Agency, an Authorization will be required.
4. Ensure utilizing most updated consent form available here: <http://211sandiego.org/community-coordination/>
5. Agency Staff must Read and/or have client read the consent or authorization
 - Client should be fully informed of risks and benefits
 - Understand how their information is shared (Notice of Privacy Practices)
 - How they can revoke consent
 - Inform the client that more information can be found at 211sandiego.org, including an updated list of 360 Community Coordination or SD United Partner Network <http://211sandiego.org/community-coordination/>
 - Upon request a copy of Authorization or Consent can be provided to the client
6. Gather a copy of the consent or authorization and upload document to SDUnited/CIE/360°:
 - a. Upload to CIE fax: 8584087517
 - b. Upload within Salesforce

Guidelines to Revoke Consent/Authorization:

In order to revoke consent, client can:

- Mail request with client name and information to Privacy Questions, PO Box 420039, San Diego, CA 92142
- Call 2-1-1 and request revoking consent

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: privacy@211sandiego.org