DATA SECURITY OVERVIEW
For RCOC Service Providers

Purpose: To prevent breaches of confidentiality.

Why: It is the law (with associated *harsh* financial penalties).

What is a breach of confidentiality?
An impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational or other harm to the affected individual.

What is NOT a breach of confidentiality?

1. Unintentional acquisition, access, or use of protected health information by a workforce member acting under the authority of a covered entity or business associate.
2. Inadvertent disclosure of protected health information from a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate.
3. If the covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

What is "Protected Health Information?"
Data are "individually identifiable" if they include any of the following types of identifiers for an individual listed below, or if the provider is aware that the information could be used, either alone or in combination with other information, to identify an individual. Different laws refer to these identifiers as "health information," "individually identifiable health information," "protected health information" and "electronic protected health information."

Confidential and personally identifiable information includes the following 19 individual identifiers:

1. **Name**
2. Address (all geographic subdivisions smaller than state, including street address, city, county, or ZIP code)
3. All elements (except years) of dates related to an individual (including birth date, admission date, discharge date, date of death, and exact age if over 89)
4. Telephone numbers
5. FAX number
6. **Social Security number**
7. **Medical record number**
8. **Health plan beneficiary number**
9. **Account number**
10. **Online Account** – User Name or Email Address, in combination with a password or

security question and answer
11. Certificate/license number
12. Any vehicle or other device serial number
13. Device identifiers or serial numbers
14. Web URL
15. IP address
16. Finger or voice prints
17. Photographic images
18. Any other unique identifying number, characteristic, or code (e.g. UCI)
19. Vehicle license plate number (effective January 2016)

NOTE: In California unauthorized disclosure of an individual's "**Name**" and any other "notice-triggering" data element **(underlined, bold)** is considered a reportable breach. In the U.S., a federally reportable breach is unauthorized disclosure of any three (of the 18 individual identifiers) data elements. (Vehicle license plate number is not a Federal personal individual identifying data element).

Reporting Protocols If A Breach Occurs

1. Notify affected individual(s) via letter
2. Submit a Security Breach Report to RCOC's Information Security Officer at iso@rcocdd.com

California law requires a state agency or business to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person.

Any person or business that is required to issue a security breach notification to more than 500 California residents as a result of a single breach shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General.

References

Federal

1. Laws: Health Insurance Portability and Accountability Act (HIPAA) & Health Information Technology for Economic and Clinical Health Act (HITECH)
2. Standards: Federal Information Processing Standards (FIPS) & National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53

State

1. Law: WIC 4514, California Civil Code section 56, California Health & Safety Code section 1280.15, Government Code section 11549.3
2. Standards: State Information Management Manual (SIMM), State Administrative Manual (SAM)

Best Practices

1. Administrative Safeguards: Policies, procedures, processes, security training, complaint

process.

2. Physical Safeguards: Locked areas, secure destruction of data, do not leave material Unattended, and don't share passwords.
3. Technical Safeguards: software to limit access, data encryption, anti-virus & malware protection.