County of San Diego, HHSA, Behavioral Health Services

Fee For Service Provider
TERM Provider

Information Privacy & Security Provisions Training

2018

OPTUM®

Information Privacy and Security Provisions

These provisions are intended to protect the privacy and security of County information that a contracted provider may create, receive, access, store, transmit, and/or destroy.

Providers should be in compliance with the following rules, regulations, and agreements as applicable:

- Health Insurance Portability and Accountability Act (HIPAA).
- County agreements with the State of California, collectively referred to as State Agreements and posted on the County's website at www.cosdcompliance.org.
- Title 42 of the Code of Federal Regulations, Chapter 1, Subchapter A, Part 2.

Providers shall use the minimum PHI required to accomplish the requirements of their contracts or as required by law. Providers may not use or disclose PHI in a manner that would violate HIPAA or any other applicable State Agreements.

OPTUM®

Confidential property of Optum. Do not distribute or reproduce without express permission from Optum.

County Protected Information

- Names
- Photographs
- Phone and Fax Numbers
- Dates (may even include year)
- Social Security numbers
- Geographic subdivisions smaller than a state
- Electronic mail (email) addresses
- Web URLs/IP addresses
- Numbers related to: medical records, health plans
- Certificate/License numbers
- Identifiers re: vehicles, devices, biometrics
- Other identifying numbers and codes
- Health/Medical Information
- Information related to Public Assistance benefits
- Computers
- Client Charts
- Client Sign-In Sheets
- Copies of Photo Identification Cards and Insurance Cards
- Case numbers
- Voicemails
- Text Messages
- Copy Machine hard drives
- Call Logs from a Cell Phone

Confidential property of Optum. Do not distribute or reproduce without express permission from Optum.

Physical Safeguards

Provider shall develop and maintain HIPAA compliant information and security program to prevent use or disclosure of County Protected Information.

- Locked offices
- Locked cabinets
- Screen savers and time outs
- Codes to identify patient names on charts or doors in facilities
- Sign-in sheets with blacked our or removal stickers for office
- Physical layout of the office to protect PHI of other patients
- Phones to be placed in back of closed window and/or door
- Workstation locations
- Fax cover sheets

Confidential property of Optum. Do not distribute or reproduce without express permission from Optum.

Data Security

Providers shall comply with data security requirements as specified by HIPAA and the State Agreements, including, but not limited to:

- Employees, interns, volunteers, subcontractors, etc., with access to County protected information shall:
  - Complete privacy training and security training to include a signed certification within thirty days of hire (30) and at least annually thereafter.
  - Sign a confidentiality statement, prior to access to County protected information.
  - Wear an identification badge at facilities that contain County protected information.
- Facilities with County protected information shall have security guards or a monitored alarm system.
- Computer warning banners for all systems containing County protected information.
- Comprehensive annual risk assessments.
- Policies and internal controls to ensure transport and storage of County protected information in cars, airplanes, trains and buses.
- Sufficient administrative, physical, and technical controls in place to protect County protected information.
- Designate a Privacy Official and a Security Official to oversee privacy and security requirements.

Confidential property of Optum. Do not distribute or reproduce without express permission from Optum.

Encryption

At Rest	Solution
Files on a computer	Encrypt hard drive
Files on a smart mobile device	Encrypt mobile device
Files on a copy machine or fax	Encrypt hard drive
Flip phones	Typically cannot encrypt; do not use for client data

In Motion	Solution
Emailing from encrypted computer	Email encryption software
Emailing/texting from smart mobile device	Email and/or text encryption software
Emailing from a copy machine	Encryption software for the copier
Faxing/phones	Nothing, good as is

Confidential property of Optum. Do not distribute or reproduce without express permission from Optum.

Breach Reporting

Providers shall report breaches and suspected privacy incidents to the County Contracting Officer's Representative and HHSA Privacy Officer.

- Initial Report:
  - Immediately Upon Discovery: Any incident that involves information related to the Social Security Administration
  - Within one (1) Business Day of the Discovery: Any suspected privacy incident or suspected breach of PHI.
- Investigation Report: Provider shall immediately investigate such suspected security incident or breach and provide the County a complete report of the investigation within seven (7) working days using County's "Privacy Incident Report" form.
- Notification: Contractor will comply with County's request to notify individuals and/or media and shall pay any costs of such notifications, as well as any costs associated with the breach. County shall approve the time, manner and content of any such notifications before notifications are made.

OPTUM®

Confidential property of Optum. Do not distribute or reproduce without express permission from Optum.

Privacy Incidents

Reportable Privacy Incidents include, *but are not limited to*:

- Misplacing a client's chart.
- Giving Client A's paperwork to Client B (even if you immediately get it back).
- Emailing a report with client information to the wrong person.
- Emailing Protected Information outside of your network in an unencrypted email (including replying to someone else's email).
- Losing a laptop, phone, or tablet.
- Mailing client documents to the wrong person.
- Throwing away client documents in the regular recycle bins.
- Copying client documents at a local copy shop (e.g. FedEx Office).
- Car stolen with client chart inside (even if car and file later found).

Confidential property of Optum. Do not distribute or reproduce without express permission from Optum.

Privacy Incident Reporting

Should a reportable privacy incident occur, please complete the following steps:

- A Privacy Incident Report must be completed and submitted to the HHSA Privacy Officer.
  - The report is submitted online: https://www.sandiegocounty.gov/content/sdc/hhsa/hhsa-priv-db.html
- Notify Optum Quality Improvement at SDQI@optum.com

Confidential property of Optum. Do not distribute or reproduce without express permission from Optum.

Mitigation and Cooperation

- Provider shall alleviate any harmful effects caused by violation of these requirements, as directed by Optum Public Sector and/or the County of San Diego.
- Providers shall provide access to PHI, as well as internal practices and records related to county PHI at the written request of Optum Public Sector or the County of San Diego within ten (10) calendar days.
- Providers will assist Optum Public Sector and/or the County of San Diego regarding a client's access, copy, amendment, accounting of disclosure, and other requests for PHI, in the time and manner designated by Optum Public Sector and/or the County of San Diego.

Confidential property of Optum. Do not distribute or reproduce without express permission from Optum.


OPTUM®