Policy and Procedure

Title/Description:	HIPAA/Privacy and Security
Approval Date:	12/10/2022
Approved By:	CEO & CMO
Version Effective Date:	03/15/2023

A. Scope:
This policy applies to all personnel of CNSL. It also applies to all business associates, contractors, vendors, temporary workers and volunteers.

B. Purpose:
CNSL must comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). HIPAA rules apply to covered entities and business associates. CNSL is a covered entity under the definitions contained in the HIPAA regulations.

CNSL is required to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, after federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. CNSL must also support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to, civil monetary penalties, criminal penalties including prison sentence, and loss of revenue and reputation from negative publicity.

Full compliance with HIPAA strengthens our ability to meet other compliance obligations and will support and strengthen our non-HIPAA compliance requirements and efforts.

Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI) and reduces the risk of breaches of confidential health data.

C. Policy and Procedures

CNSL obtains most of its PHI from patients through care applications, assessments, and direct questions. CNSL may also obtain PHI from community health care agencies, other governmental agencies or health care providers.

CNSL shall provide patients with a copy of its HIPAA Notice of Privacy Practices during patient registration. A copy of this Notice shall also be available on CNSL's web-site.

Permitted Uses and Disclosures:

CNSL is permitted to disclose PHI for the following purposes:

1) Treatment – CNSL may use or disclose PHI to physicians, psychologists, nurses, and other authorized healthcare professionals who need PHI in order to conduct an examination, prescribe medication, or otherwise provide treatment to a patient.
2) To Obtain Payment – CNSL may use or disclose PHI to insurance companies, government agencies, or health plans assist CNSL in obtaining payment for services rendered.
3) For Health Care Operations – CNSL may use or disclose PHI in the course of activities necessary to support health care operations, such as performing quality checks on employee services. PHI may also be disclosed to Business Associates who assist in the performance of health services; Business Associates must have an executed Business Associate Agreement.

Other permitted disclosures include when required by law, for public health activities, for health oversight activities, to avert serious threat to health and safety, to personal representatives, and to family and friends. Disclosures for any reason other than for treatment, payment, or health care operations require an appropriate authorization by the patient or the approval of CNSL's Chief Executive Officer.

Incidental uses and disclosures are those that cannot be reasonably prevented, are limited in nature and that occur as a by-product of a permitted use or disclosure. Such incidental uses and disclosures are permitted as long as CNSL uses reasonable safeguards and use or disclose only the minimum amount of PHI necessary.

PHI Disclosures in Accordance with Law:

PHI may be provided in accordance with law when required by subpoena, court order, or other law enforcement disclosures. All such requests must be directed to CNSL's CEO.

Documentation of Disclosures:

All disclosures, except for those permitted by law for treatment, payment, and health care operations, shall be documented in the patient's medical record.

Minimum Necessary Standard:

For all disclosures, CNSL personnel shall only access, transmit, or handle the minimum amount of PHI that is necessary to perform a given task.

Verification of Identity and Authority:

Before sharing patient PHI with a third party, CNSL personnel must verify the identify of the receiving party. If the receiving party is another Covered Entity, personnel must verify the tax ID and NPI of the

requestor. If the receiving party is not a Covered Entity, a Business Associate Agreement must be executed, or the patient must have an appropriate signed release on file permitting release of information to the receiving party.

Business Associate Agreements:

A Business Associate Agreement (BAA) must be executed with any contractor/subcontractor or vendor prior to the sharing of any PHI. Contact CNSL's CEO if a BAA is needed or to verify if a BAA is already in place prior to sharing PHI with any contractor/subcontractor or vendor. When contacting CNSL's Ceo, identify the proposed use and disclosure of PHI and define under what circumstances the BAA must specify each party's responsibilities when it comes to PHI. The BAA must also include the 42 CFR, Part 2 information within the BAA or as a separate form to be signed by both parties.

Training of Personnel:

Demonstrated competence in the requirement of the policy is an important part of the responsibilities of every member of the workforce. Employee training shall occur for all new hires during Orientation and before new hires engage with patients per GA state rule.

Human Resources shall, at a minimum provides training to all employees. HR shall also implement an email policy of sending minimum, necessary information to acknowledged person(s) for the acknowledged purpose. Patient identifier is first name of patient, Last Initial. All CNSL emails are encrypted with the 42 CFR, Part 2 message at the end of each email. HR is responsible for educating staff of potential threats of breaches of security regarding all HIPAA laws and regulations. Human Resources is responsible for compliance of employees and any violations of HIPAA intentionally or unintentionally for corrective action plans and/or could lead up to termination of employment.

CNSL Human Resources will develop a HIPAA refresher course that will address any updates that will affect employee compliance.

Breach Reporting:

HIPAA Security Breach checklist includes Breach Notification and summary of how a breach may be discovered, state the nature and extent of PHI involved, detail the unauthorized person to whom the disclosure was made, determine whether the (PHI) was acquired or viewed, determine if 500 or more individuals were affected and breach is correctly identified such as loss, theft, exposure, or impermissible disclosure of healthcare records.

Security:

CNSL shall perform an annual Risk Assessment. Clinical areas are required to ensure no PHI is visible or accessible to any person(s) entering office space. Any PHI must be turned over or placed on the desk of any employee and out of the sight of any other employees, visitors or vendors. Computers are to be positioned so screens are not visible to others and are timed with screen savers after a period of time. All employee computers are secured with our IT department with passwords that change after a set period of time and two-factor authentication. Medical records are stored in an EMR and are only accessible for staff on a basis of need

to know, and individual passwords are required to access the EMR. Only Super Administrators have full access to all medical records with password protection.

Safeguards:

HIPAA Data Back Up: CNSL IT identifies the database containing ePHI, identifies email systems containing ePHI, determines risk level of each file, and backs up data daily. Testing and restoring systems if needed.

HIPAA Omnibus Rule: This rule was introduced in 2013 as a way to amend the HIPAA privacy and security rules requirements, including changes to the obligations of business associates regarding the management of PHI. The rules merges the following four separate rule makings: amendments to HIPAA Privacy and Security rules requirements, HIPAA and HIPAA Privacy and Security rules requirements, HIPAA and HIPAA HITECH under one rule, further requirements for data breach notifications and penalty enforcement, approving the regulations in regards to the HITECH Act's breach notification rule, manage the use of patient information in marketing, includes a provision that requires healthcare providers to report data breaches that are deemed not harmful, makes certain that business associates and subcontractors are liable for their own breaches and requires Business Associates to comply with HIPAA.

Individual Rights Under HIPAA:

- **Access to Certain Records:** Patients have the right to inspect and copy their PHI in a designated record set except where State law may prohibit access. A designated record set contains medical and billing and case management information. If CNSL does not have the patient's PHI record set but know who does, we will inform you how to get it. If CNSL's PHI is a copy of information maintained by another health care provider, CNSL may direct the patient to request the PHI from them. If CNSL denies the patient's request for access to information (which should be reviewed/approved by CNSL's CEO), the patient has the right to ask for the denial to be reviewed by another healthcare professional designated by CNSL.
- **Amendments to Certain Records:** Patients have the right to request certain amendments to their PHI if, for example, they believe a mistake has been made or a vital piece of information is missing. CNSL is not required to make the requested amendments and must inform the patient in writing of its response.
- **Accounting of Disclosures:** Patients have the right to receive an accounting of disclosures of their PHI that were made by CNSL for a period of six (6) years prior to the date of their written request. This accounting does not include for purposes of treatment, payment, health care operations or certain other excluded purposes, but includes other types of disclosures, including disclosures for public health purposes or in response to a subpoena or court order.
- **Restrictions:** Patient have the right to request that CNSL agree to restrictions on certain uses and disclosures of PHI, but is not required to agree to the request. Patients cannot place limits on uses and disclosures that CNSL is legally required or allowed to make.
- **Revoke Authorizations:** Patients have the right to revoke any authorizations they have provided, except to the extent that CNSL has already relied upon the prior authorization.

- **Delivery by Alternate Means or Alternate Address:** Patients have the right to request that CNSL send PHI by alternate means or to an alternate address.
- **Complaints & How to Contact Us:** If a patient believes their privacy rights have been violated, they have the right to file a complaint by contacting CNSL at the address and/or phone number indicated below. They also have the right to file a complaint with the Secretary of the United States Department of Health and Human services in Washington, D.C. CNSL will not retaliate against patients for filing a complaint.

If a patient believes their privacy rights have been violated, they may make a complaint by contacting Daniel Harvey, CEO, at 678-384-4911 or the Secretary for the Department of Health and Human Services. No individual will be retaliated against for filing a complaint.

The U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201
Toll Free: 1-877-696-6775

Patients have the right and choice to tell CNSL how/whether to share information with family, close friends, or others involved in their care, share information in a disaster relief situation, and include information in a CNSL directory. This information should be documented in the patient's medical record.

D. DEFINITIONS

a. **Business Associate** – A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or providers services to, a covered entity. A member of the covered entity's workforce is not a business associate.

b. **BAA (Business Associate Agreement**) – A covered entity's contract or other written arrangement with its business associate must contain the elements specified at 45 CFR 164.504(e). For example, the contract must: Describe the permitted and required uses of protected health information by the business associate; Provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law; and require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract.

c. **Covered Entity** – An individual, organization or agency who/which must comply with HIPAA. Health plans, clearinghouses, and health care providers who submit HIPAA transactions, like claims, electronically are covered entities.

d. **HIPAA** – The Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act, and their implementing regulations set forth at 45 C.F.R. Parts 160-164. HIPAA is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed with the patient's consent or knowledge.

e. **PHI** – PHI stands for Protected Health Information. PHI is any health information that can be tied to an individual. PHI includes: names; all geographical indicators smaller than a state (except for the first 3 digits of a zip code), dates directly related to an individual, phone/fax numbers, email

addresses, social security numbers, medical record numbers, health insurance beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers and serial numbers, device identifiers and serial number, URLs, IP address numbers, biometric identifiers, any other unique identifying number, characteristic or code, and full face photographic images and any comparable images. PHI only relates to information on patients or health plan members.

E. SOURCES AND REFERENCES

1. www.hhs.gov
2. www.cdc.gov