Overview of NLACRC’s Contractual Requirements with DDS to Comply With Privacy Laws

NLACRC is required to follow Federal & State laws regarding HIPAA, whichever is more restrictive.

NLACRC is required to ensure all Service Providers comply with the same restrictions, safeguards, and conditions that apply to NLACRC with respect to protected health information.
HIPAA HISTORICAL BACKGROUND

• The Health Insurance Portability and Accountability Act ("HIPAA") was enacted by the United States Congress and signed by President Bill Clinton in 1996.

• This law was enacted as part of a broad congressional attempt at incremental healthcare reform.
The HIPAA Privacy Rule

The HIPAA Privacy Rule ("Rule") establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.

The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.

The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.
Privacy Rule vs. Security Rule

• The Privacy Rule sets the standards for, among other things, who may have access to Protected Health Information (“PHI”), while the Security Rule sets the standards for ensuring that only those who should have access to PHI will actually have access.

• The Privacy Rule also applies to all forms of consumer PHI, whether electronic, written, or oral. In contrast, the Security Rule covers only protected health information that is in electronic form. This includes EPHI that is created, received, maintained or transmitted. For example, EPHI may be transmitted over the Internet, stored on a computer, a CD, a disk, magnetic tape, or other related means.
Important Definitions in the Privacy Rule

• **Covered Entity (DDS):**
  o A health plan.
  o A health care clearinghouse.
  o A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

• **Business Associate (NLACRC):**
  o An entity that creates, receives, maintains, or transmits protected health information on behalf of a covered entity.
  o Includes claims processing or administration, data analysis, processing, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, repricing, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

• **Subcontractor (Service Providers):**
  o A person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.
PHI vs. EPHI?

• Individually identifiable protected health information ("PHI") is information, including demographic data, that relates to:
  o The individual’s past, present or future physical or mental health or condition
  o The provision of health care to the individual, or
  o The past, present, or future payment of the provision of health care to the individual
  o And that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.

• ("EPHI") is individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.
### Examples of PHI

- Names
- Addresses
- Geographic subdivisions smaller than State
- Dates directly related to an individual (Date of Birth)
- Telephone numbers
- Fax numbers
- Email addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/License Numbers

- Vehicle identifiers and serial numbers
- URLs
- IP address numbers
- Biometric identifiers, including finger/voice prints
- Full face photographic images
- Any medical information obtained from an individual's medical record
- Medi-Cal Number
- Diagnosis
- Drivers License
- Financial Information, such as bank account or tax return
Minimum Necessary

• Service Providers are required to make reasonable efforts to limit the use or disclosure of PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

• Service Providers may use or disclose PHI only to perform functions, activities, or services for or on behalf of a consumer.

• Service providers may disclose PHI if necessary for the legal, management, or administrative purposes of the service provider.
  o In disclosing PHI, service provider disclosure must be required by law or the service provider must obtain reasonable assurances the PHI will remain confidential and used or further disclosed by law or for the purpose for which the PHI was disclosed and the recipient notifies service provider of any instances that confidentiality has been breached.
Uses and Disclosures

- Service Providers May Not use or disclose PHI, except as permitted or required.
- Does Not Apply to:
  - Disclosures to or requests by NLACRC or DDS
  - Uses or disclosures made to the consumer
  - Uses or disclosures made pursuant to an authorization
  - Disclosures made to the Secretary of Health & Human Services during investigation of HIPAA Compliance
  - Uses or disclosures that are required by law
  - Uses or disclosures that are required for compliance with HIPAA
Compliance Review

- Service Providers shall make its internal practices, books and records relating to the use and disclosure of PHI received from NLACRC, or created or received by service provider on behalf of NLACRC, available to NLACRC, DDS or the Secretary for purposes of investigating or auditing compliance with the requirements of HIPAA regulations and the HITECH Act.
The HIPAA Security Rule

• The HIPAA Security Rule establishes national standards to protect individuals’ electronic PHI that is created, received, used, or maintained by a covered entity.

• The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI.
Safeguarding Requirements

- Service Provider shall implement administrative, physical and technical safeguards that reasonably protect the confidentiality, integrity, and availability of the PHI, including electronic (digitized) PHI it creates, receives, maintains and transmits in an electronic form to prevent unauthorized access, viewing, use, disclosure or breach of PHI.

- Requires the removal of PHI and the protection of PHI data.
• Service Provider shall ensure all computerized data systems containing PHI are in compliance with HIPAA and HITECH Act.

1. Ensure appropriate security levels to maintain confidentiality, integrity and availability of PHI and electronic PHI.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of PHI and electronic PHI.
3. Protect against any reasonably anticipated uses of disclosures of PHI and electronic PHI that are not permitted or requested.
4. Require encryption of PHI that is confidential, sensitive and personal when it is stored or transmitted using portable computing devices and/or portable electronic storage media.
Administrative Safeguards

- Risk Assessment
- Policies and Procedures
- Security training requirements of employees
- Information access management
- Incident Response Plan
- Disaster Recovery Plan
- Business Associate Agreements with your sub-contractors
- Assignment or delegation of security responsibility to an individual(s)
- Business Associate Contracts
- Audit controls
Physical Safeguards

- Security Systems
- Fire Alarms
- Locked Doors
- Locked Storage
- Inventory of Assets with PHI data
- Retaining off site computer backups
- Workstation security
- Device and media controls
Technical Safeguards

• Access Controls – Unique Logins, Secure Passwords or Pass Phrases, Two Factor Authentication, least access
• Firewalls
• Intrusion Detection and/or Prevention
• Encryption for laptops, phones, flash drives and anything leaving the office
• Secure transmission of EPHI data
• Secure email transmission
• Retaining off site computer backups
• Workstation security
• Antivirus/Malware
• Device and media controls
What are we Protecting Against?

• Accidental disclosure of PHI data to unauthorized people
• Insecure storage
• Insecure sending
• Unauthorized viewing
• Unreliable data due to integrity control issues
• Data loss due to a disaster or inability to recover from backups
• Subcontractors creating a breach because of lack of knowledge of HIPAA and security in general
• Hackers who want to steal data, identities, etc
The Threat is REAL

• NLACRC recent attacks
  o Attack on our website coordinated from France, Netherlands, Vietnam
  o Phishing email from one of our vendors who was compromised
  o Attack on our website

• Attacks in the news
  o DocuSign
  o WanaCrypt

• #getserious #orgethacked
NLACRC Strategy – Technology

• Defense in Depth
  • Intrusion Detection – Collects traffic and scans for malicious addresses and traffic patterns. Info that is reviewed by security personnel – response time 15 minutes

• Firewalls – prevent unauthorized traffic

• Anti-virus – Looks for signatures associated with viruses

• Backup and Disaster Recovery – Restoration of damaged and deleted files

• Mobile Device Management – Compartmentalizes work data, controls access
**NLACRC Strategy – People**

- Network Login Passwords – Unique and not shared
- Application Passwords – Not shared between sites
- Encryption – Anything that leaves electronically needs to be encrypted
- Enhanced training about security and threats
- Vendors at every level trained and educated
HIPAA BREACHES

How to Identify and Respond to Breach Situations
What is a “Breach” or Unauthorized Disclosure?

- Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted, which compromises the security or privacy of the protected health information.

- The unauthorized release, transfer, provision of unauthorized access to, or divulging in any manner of information outside the service provider holding the information.
Breach Examples

• Mailing information with PHI to the incorrect recipient
• Emailing, unencrypted information with PHI to the incorrect recipient(s)
• Unauthorized access to computer or server containing PHI
• Unauthorized access or loss of an unencrypted portable device, containing PHI, including but not limited to phones, iPads, notepads, laptops, thumb drives, flash drives, etc
**Breach Obligation: Notification**

- Service Provider must notify NLACRC within **24** hours of the discovery of the breach*
- NLACRC must notify DDS within **72** hours of discovery of the breach
- Service Providers must notify the affected individuals in writing within 60 days of the discovery of the breach:
  - If deceased, next of kin must be notified
  - If no contact information, substitute notice must be provided
- DDS must notify the Office for Civil Rights (OCR):
  - If more than 500 individuals affected by the breach, within 60 days
  - If less than 500 individuals affected by the breach, within 60 days of the end of the calendar year
- Must notify the media if more than 500 individuals affected by the breach

*Note: There may be additional requirements or exceptions not listed here.*
Information to be Provided to NLACRC Within 24 Hours

1. Date of incident
2. What happened
3. List of all PHI that was disclosed
4. Name(s) of consumers and/or family members
5. UCI(s) of consumers and/or family members
Information to be Provided to NLACRC Within 72 Hours

1. Copy of Police Report, if applicable
2. Copy of Breach Notification letter to each consumer and/or family member (must be performed within 30 days)
3. Amount of cost incurred by service provider to address the breach (credit monitoring, legal fees etc.)
4. Name of service provider’s Privacy Officer and Security Officer
5. Action service provider is taking to mitigate a similar privacy breach in the future.
6. Completed and signed SIMM 5340 report
Accounting Of Breaches

• Maintain a record (accounting) of all PHI disclosures by individual for six years.
OCR Breach Investigations

If the evidence indicates that the service provider was not in compliance, OCR will attempt to resolve the case with the covered entity by obtaining:

- Voluntary compliance;
- Corrective action; and/or
- Resolution agreement

If the service provider does not take action to resolve the matter in a way that is satisfactory, OCR may decide to impose civil money penalties on the covered entity.

If monetary penalties are imposed, the service provider may request a hearing in which an HHS administrative law judge decides if the penalties are supported by the evidence in the case.

Complainants do not receive a portion of monetary penalties collected from covered entities.
## Potential Penalties

<table>
<thead>
<tr>
<th>HIPAA Violation</th>
<th>Minimum Penalty</th>
<th>Maximum Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA</td>
<td>$100 per violation, with an annual maximum of $25,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation due to reasonable cause and not due to willful neglect</td>
<td>$1,000 per violation, with an annual maximum of $100,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation due to willful neglect but violation is corrected within the required time period</td>
<td>$10,000 per violation, with an annual maximum of $250,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation is due to willful neglect and is not corrected</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
</tbody>
</table>

*45 C.F.R. §160.404*
Actions Upon Termination of Vendorization

- Service Providers shall return all PHI, including electronic records to NLACRC that they have in their possession.
- Service Provider must demonstrate all PHI in their possession is destroyed.
We highly encourage you to seek out an expert in the field of HIPAA to ensure compliance with the Federal and State privacy laws.