State of New Hampshire

GENERAL COURT

CONCORD

MEMORANDUM

DATE: **November 1, 2021**

TO: **Honorable Sherman Packard, Speaker of the House**
Honorable Chuck Morse, President of the Senate
Honorable Paul C. Smith, House Clerk
Honorable Tammy L. Wright, Senate Clerk
Honorable Chris Sununu, Governor
Michael York, State Librarian

FROM: **Representative Mark Pearson, Chairman**

SUBJECT: **Final Report of the Commission Relative to the Closed Loop ReferralSystem** (HB 2, Chapter 0091, Section 331, Laws of 2021)

Pursuant to HB 2, Chapter 91, section 331, Laws of 2021, enclosed please find the final report ofthe Health & Human Services Oversight Committee's comprehensive review of the Closed LoopReferral System procured by the Department of Health & Human Services.

Should you have any questions, please do not hesitate to contact the Committee. I'd like to thankmembers of the Committee, members of the Department of Health & Human Services, and the public for assisting the Committee with this review.

Enclosures

cc: Members of the Senate Health and Human Services Committee
Members of the House Health, Human Services and Elderly Affairs Committee
Members of the SenateFinance Committee
Members of House Finance Committee

Final Report

of the Health & Human Services Oversight Committee on the Closed Loop Referral System procured by the Department of Health & Human Services

November 1, 2021

I. BACKGROUND

A. Bottom Line Up Front

This report was required by 2021 HB2 language reading in part (sub numbers added for ease of reading):

"91:331 Department of Health and Human Services; Closed Loop Referral System. (1) Notwithstanding any other provision of the law to the contrary, there shall be no further expansion of the "closed loop referral" system by the department of health and human services beyond that which has been or will be implemented pursuant to the sole source grant agreement to Unite USA Inc. of Nashua in the amount of $700,000 dated October 19, 2020. (2) Before the department undertakes any further utilization of the closed loop referral system beyond that authorized by the preceding sentence, the legislative oversight committee on health and human services, established in RSA 126-A:13, shall conduct a comprehensive review of the information intended to be stored in the master index file or accessed using the master indexes within and between the closed loop referral system and other interconnected systems. (3) Further, the oversight committee shall assess the privacy protections and access/release limitations afforded by this system, and the adequacy of the procedures utilized by the system to insure that persons

using it have given informed consent to the ("opt-in") release of their personally identifiable information available through the system of systems. The department shall provide all requested data and information regarding the closed loop referral system and systems with which it is intended to interconnect within one week of the request by the oversight committee. The oversight committee shall report its findings and recommendations, if any, to the legislature, the governor, and the department of health and human services by November 1, 2021. (4a) The department of health and human services is prohibited from accessing an individual's information from the closed loop referral system who is not receiving services funded through a department of health and human services program. shall begin the process of notification by first class mail to all individuals impacted by the data breach. (4c) Any individual whose information is intended to be included in the closed loop referral shall retain the right to opt into the system on each referral and retain the right to revoke consent to be in the system at any time."

- To comply with the first requirement (1), correspondence from the Senate raised issues regarding the legislative intent related to the Department's continuing use of Closed Loop System contract. Subsequently in conjunction with Attorney General advice, the Department ceased execution of the Unite USA contract and did not use any of the options within the contract to extend work. The contract terminated September 30, 2021, by its own terms and based on the restrictions in HB 2, the Department did not move forward with a contract at this time. The department is not engaged with Unite USA Inc. beyond final discussions surrounding termination of the contract.

- The second requirement (2) generates the need for this report by the HHS Oversight Committee to conduct "a comprehensive review of the information intended to be stored in the master index file or accessed using the master indexes within and between the closed loop referral system and other interconnected systems." Unite USA did not provide the Data Dictionaries, Use Cases and/or User Training Screen Shots which would have facilitated a comprehensive review. The Department supplemented the materials by providing a data element list found in an annex. While Unite USA did provide self-described "sensitive" New User Training Materials showing design concepts and limited screen shots, these materials were insufficient to assess data flows within and between networked systems. The Department supplemented the materials by providing a data element list found in an annex. **Based solely on what's been provided, the Committee is unable to reach a decision on whether the master index file and access to the system creates an unusually significant privacy risk.** There are data elements that one

might expect that are not included in the materials provided. Data such as income, Medicaid status, and veteran status are not listed. The point of mentioning some examples of data not included is that it may suggest either that data has not been identified as part of this inquiry or alternatively, a more minimal data set is what is truly being used.

- The third requirement (3) directed the HHS Oversight Committee to "assess the privacy protections and access/release limitations afforded by this system, and the adequacy of the procedures utilized by the system to insure those persons using it have given informed consent to the ("opt-in") release of their personally identifiable information available through the system of systems." This third requirement has been partially completed. In the opinion of the committee members, the Department has an array of activities embedded throughout their IT Project Management methodologies that tend to ensure privacy considerations are included. The Department should continue to adopt "Privacy by Design" as a core philosophy for ensuring a systemic, fully integrated, set of approaches that work together to drive high levels of privacy assurance within the Department and among external partners. That systemic Privacy by Design philosophy is not fully implemented across the Department and the Closed Loop Referral System is likely one of many IT implementations that have proceeded to Go-Live in a less structured environment. This comment should not be taken to imply that the Department has allowed privacy or security vulnerabilities. Rather, it is meant to identify a potential systemic weakness that ought to be addressed in a manner consistent with industry best practices. Specific recommendations to close the key strategic gaps are listed elsewhere but generally include Privacy Governance, Privacy Policy, Privacy Maturity Models, Risk Management (Privacy Impact Assessments), Opt-in, simple written and comprehensive data sharing agreements. Legislation has been submitted in LSR 2022-2019.

- The fourth requirement included initial policies on privacy in a Closed Loop Referral System that will require legislation if the policies are to be made permanent. Members of this committee intend to file such legislation. A Senate Bill has been submitted.

B. Legislative History

The Closed Loop System is a complex database system designed to enhance care coordination by connecting clients to services through managed referrals and, upon informed consent, to share their personal information through a database of networked providers. The Department of Health and Human Services procured the initial closed loop referral system with a scope limited to substance abuse services in October of 2020 during the global pandemic. Due to the State of Emergency,

legislative and Executive Council involvement were not required for approval. The agency procured the system as a sole source contract with Unite Us. This sole source decision was made as a permissible exception to RSA 21-I:11 requiring competitive bids in routine contracting actions. This initial system was federally funded at a cost of approximately $700,000 and included up to three additional options to extend deliverables beyond the primary scope of work.

Expansion of the Closed Loop Referral System beyond the initial scope was requested by the Department through the 2021 capital budget process. The expansion was valued at over $8 million dollars including $2,682,240.00 in state dollars to match $5,445,760.00 of federal dollars to expand the referral database system statewide. The request was not funded by the legislature. Privacy and procurement concerns about the closed loop referral system were initially raised in the legislature through House Bill 601 (2021 session), sponsored by Rep. Keith Ammon, Rep. Michael Sylvia, Rep. Jeanine Notter and Senator Gary Daniels, but the specific policy provisions contained in HB 601 were deemed not ready for passage by the House Health, Human Services and Elderly Affairs Committee. The House Finance Committee reviewed the issue and determined a comprehensive review by the HHS Oversight Committee was necessary before any further expansion of the database was undertaken. House Finance added language to address the issue in HB 2. The Senate Finance Committee amended the language in HB 2 to include several policy provisions for the existing closed loop system and required the report by this oversight committee be submitted by November 1, 2021. The Senate language was adopted in conference committee and the Governor signed HB 2 on June 25th, 2021 with an effective date of July 1, 2021.

B. Issues Raised

- Privacy & the NH Constitution

In 2018, New Hampshire voters overwhelmingly approved an amendment to the State's constitution regarding privacy. The amendment was passed by 81% of the voters. The Amendment reads:

> "Right to Privacy: An individual's right to live free from governmental intrusion in private or personal information is natural, essential and inherent."

The passage of this constitutional amendment represents a fundamental shift in the expectations the public has regarding the state’s duty to protect the privacy of its citizens, including the way state agencies protect and/or avoid collection of

personally identifiable information (PII)[1]. Court cases may further establish additional protections relative to other demographic data of its citizens. In an age where technology is ubiquitous, information gathering is intrinsic, data sharing is too often assumed and data mining can achieve Orwellian profiles on individuals, New Hampshire voters have chosen a path of privacy protection.

- Privacy Culture

  Meeting our citizen's privacy expectations requires the proactive development of a culture of privacy supported by a vigilant Executive Branch and Legislature. Over time, state agencies would reasonably be expected to evolve enhanced personal privacy protection. The evolving culture will adopt "privacy by design" in our thought leadership. It is common for organizations to use a Privacy Maturity Model[2] (such as the following example from Mitre) to develop an initial baseline and then to establish measurable objectives to attain higher levels of information security and privacy.

[1] The Department of Homeland Security (DHS) defines personally identifiable information, or PII, as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

[2] Privacy Maturity Model Version 1 (mitre.org)

Element	Description
1.0: Leadership & Organization	Providing organizational support for privacy program priorities and initiatives
2.0: Privacy Risk Management	Using methods and processes to identify, assess, prioritize, and manage privacy risk, including within IT investment, acquisition, and contract management processes.
3.0: Engineering & Information Security	Incorporating privacy into the enterprise systems engineering approach and integrating with cybersecurity
4.0: Incident Response	Managing and responding to privacy incidents, including breaches
5.0: Individual Participation, Transparency & Redress	Informing data subjects and the public regarding information about individuals the organization collects and uses, and how the public may pursue inquiries and complaints

[1] Based on a Federal CIO Council Privacy Committee White Paper entitled *Best Practices: Elements of a Federal Privacy Program,* June 30, 2010

6.0: Privacy Training & Awareness	Establishing and maintaining workforce training and a culture of privacy awareness
7.0: Accountability	Enforcing the responsibility of the organization to implement privacy principles and requirements and to respond to concerns expressed by individuals and the general public

The voters of New Hampshire clearly stated the need for a culture of privacy for personal information and the Legislature needs to adhere to the culture as it moves towards creating new policies. While we have laws which seek to improve the state's public health and well-being, we need to be vigilant that any new programs and/or policies adhere to the constitutional right to privacy. The balance must always be tilted towards the constitutional privacy requirement.

- Best Practices in Privacy Policy and Internet Data Security.

  Key to any type of data collection by the State are best practices in privacy policy and data security. If the process for protecting personal information is not clearly defined, the risk of data breach increases. There are federal and state laws governing privacy, yet with every new program a review (Privacy Impact Assessment) should be undertaken to make sure that personal information is protected and the ongoing process for protection is strong. Ongoing review and assessments are necessary as the risk environment changes and creates new risks to personal privacy when personal information is kept by the State in a database.

- CMS Waiver.

  In the Senate, there were assertions made that certain federal waivers require a closed loop referral system developed by the State. Clarity of these assertions was requested, as well as review of other state waivers and current state programs (ex. managed care organization referral systems) to determine what is necessary and what could be seen as duplicative. Managed Care Organizations contracting with the State to manage the health and well-being of the Medicaid population are required to have a closed loop referral process. This requirement of managed care organizations on behalf of Medicaid members apply to both health providers and social services. The question of how this system differs from what is currently in place needs more research to avoid duplication. If the State moves forward to expand the closed loop referral system beyond the managed care organizations and the Medicaid population, the need for privacy protections and security compliance is critical.

- Method of Procurement.

  The expedited procurement of the system led to questions about thorough review and cost effectiveness. There was no competitive solicitation. In general, for programs of this nature, legislative and executive council reviews are common. Competitive bidding is often required to make sure the State receives the lowest cost and best value for taxpayer funds for any program and this program should be no exception.

The Health & Human Services Oversight Committee examined these issues in concert with the Department of Health & Human Services and other interested stakeholders. The goal was to determine the level of privacy and confidentiality afforded to the state's citizens in their personal interactions with the many state, local, non-profit and for-profit health and social service providers through a Closed Loop Referral System.

II. Oversight Committee Review

The chronology of Oversight Committee agenda item discussions, Committee member inquiries, and various efforts to gather information are available to the public on the Committee's webpage under "Agendas," "Minutes," and "Documents."

Statutory and Study Committee Search (state.nh.us)

The Committee Chair tasked members Edwards, Rosenwald, and Giuda to seek out information during the summer months for review of the Committee in the fall. Meetings and discussions with DHHS and other stakeholders, including closed loop referral system vendors, were held. Several documents, including information from the Department about the Closed Loop referral process, including the areas of Governance, Acquisition, Implementation, and Individual/Client Privacy, are published on the Committee website. Review of other RSA's concerning privacy in New Hampshire are included in the Appendix.

III. Findings and Recommendations

If a Closed Loop Referral System is pursued, the system will add significant information privacy risk due to the dramatic increase of sharing of NH citizen's personal information across disparate, loosely connected organizations without effective control of personnel training and discipline of agents from community organizations. The Committee's review of the Closed Loop Referral System has led to a range of additional approaches to enhance risk mitigation. One such approach is to follow a formal Request for Proposal contracting methodology fully to identify competitive privacy and IT Security architectures and techniques. The external personnel risks remain and mitigations must be identified and implemented.

Future RFPs or engagements should require screen shots and Use Cases so that DHHS can ensure there is no significant risk to the data privacy of participating NH citizens.

The Committee also finds that a stronger privacy culture supported by internal governance are needed at DHHS to enhance personal privacy protection. The Committee recommends legislation be filed in 2022 to establish improved governance in the Department and to establish and enhance policies for the clear and transparent protection of personal privacy of individuals whose information would be kept in a closed loop referral system.

Below are the issues that are recommended for future legislation in more detail:

DHHS Privacy Governance/ Privacy Maturity Models

The Department needs strong governance for privacy of personal information. Gaps exist in the governance for protecting personal information. While there are federal laws and state laws that require certain medical information to be protected under HIPAA, the process for personal privacy in the Department could be improved. Also, with the new effort to collect personal information specific to social services which are not protected by HIPAA, DHHS should develop a privacy structure that has benchmarks, compliance reviews, data governance documents and clear policies. Other state agencies, like the Department of Safety, have privacy committees established by law to make sure the personal information of the citizenry is protected. The Legislature should consider legislating the formation of such a committee at DHHS to guide the governance of data at the Department.

Privacy Impact Assessments/Risk Management

In the data security industry, Privacy Impact Assessments are a common tool to assure quality of the system and the process needed to advance privacy protection. DHHS is in the process of a Privacy Impact Assessment for the limited Closed Loop Referral system in place. There is a need to implement quality assurance measures related to Privacy Impact Assessment prior to any "go-live" of the system. In data security, there are several standards organization that can be followed. Often, the International Organization for Standardization (ISO) is commonly referred to. In terms of data security, a preferred standards organization for DHHS to follow is the Healthcare Information and Management Systems Society (HIMSS).

Privacy Policy / How Much Data should be Collected?

In carrying out its duties, the department should use the minimum amount of information that is reasonably necessary to serve and protect the health of the public. As the Closed Loop Referral system also includes social service data which goes beyond protected health information under HIPAA, there should be legislative approval required for the collection of non-HIPAA protected data if it is determined to be needed. If the data collection is allowed under law, there needs to be a stronger process in place to manage and protect that personal information, including who has access. The Legislature should establish that DHHS shall not access information on individuals that are not receiving financial benefits from DHHS. (Note: language in HB 2)

Opt In / Opt Out.

With the passage of the constitutional amendment on personal privacy, it is the Committee's recommendation for individuals to retain the right to "Opt In" on each referral for any individual whose information is intended to be included in a closed loop referral database. Language that was passed in House Bill 2 relative to this right should be reviewed and submitted for permanent inclusion in the statutes. Individuals should also retain the right to revoke consent to be in the system at any time. While there are federal guidelines as to the length of time personal health information must be kept, the Legislature should consider establishing a provision in law which requires removal of personal non-health identifiable information from the database consistent with state and federal data retention requirements. There should be no adverse consequences for individuals (i.e. denial of service) who choose not to opt in.

Uniform Consent

A standardized Uniform Consent form for individuals should be clearly written in plain language and required at each referral for inclusion in the database. The language of the uniform consent should be approved by the Health & Human Services Oversight Committee.

Prohibitions & Enforcement

Certain policies relative to protecting the personal information from bad actors or other inadvertent disclosures should be reviewed. A policy prohibiting vendors, business associates or network participants from selling or marketing personal information by individuals who have accessed the database and/or are included in the database is recommended. A policy prohibiting network participants from accessing personal information from the closed loop referral system other than with respect to those individuals who have been referred to it for services and have become a client is also recommended. The Committee recommends DHHS adopt formal controls prohibiting both activities. Persons who knowingly violate such policies should be subjected to criminal penalties.

Competitive Bidding/Procurement.

With the pandemic behind us, the process of competitive bidding should be required for any future use or expansion of a closed loop referral system.

The Committee urges DHHS to include all recommendations on privacy and security from HB 2 along with recommendations of the Privacy Impact Assessment if it intends to continue to contract on a closed loop referral system with a private vendor.

Appendix

I. HB 2, Chapter 91, section 331, Laws of 2021

331 Department of Health and Human Services; Closed Loop Referral System. Notwithstanding any other provision of the law to the contrary, there shall be no further expansion of the "closed loop referral" system by the department of health and human services beyond that which has been or will be implemented pursuant to the sole source grant agreement to Unite USA Inc. of Nashua in the amount of $700,000 dated October 19, 2020. Before the department undertakes any further utilization of the closed loop referral system beyond that authorized by the preceding sentence, the legislative oversight committee on health and human services, established in RSA 126-A:13, shall conduct a comprehensive review of the information intended to be stored in the master index file or accessed using the master indexes within and between the closed loop referral system and other interconnected systems. Further, the oversight committee shall assess the privacy protections and access/release limitations afforded by this system, and the adequacy of the procedures utilized by the system to insure that persons using it have given informed consent to the ("opt-in") release of their personally identifiable information available through the system of systems. The department shall provide all requested data and information regarding the closed loop referral system and systems with which it is intended to interconnect within one week of the request by the oversight committee. The oversight committee shall report its findings and recommendations, if any, to the legislature, the governor, and the department of health and human services by November 1, 2021. The department of health and human services is prohibited from accessing an individual's information from the closed loop referral system who is not receiving services funded through a department of health and human services program. Within 48 hours of becoming aware of a data breach, Unite USA Inc. shall begin the process of notification by first class mail to all individuals impacted by the data breach. Any individual whose information is intended to be included in the closed loop referral shall retain the right to opt in to the system on each referral and retain the right to revoke consent to be in the system at any time.

II. **Additional information to understand the data collected are the following high level fields (not all are required and a referral could be made with partial completion**):

1. Date of Birth
2. Ethnicity
3. First and Last Name
4. Gender
5. Marital Status
6. Race
7. City
8. State
9. Zip Code
10. County
11. Country
12. Email
13. Insurance information
14. Phone number

III. Examples of New Hampshire RSA's specific to privacy/databases

New Hampshire RSA's. A brief search of privacy related laws in New Hampshire results in specific privacy laws pertaining to collection and management of personal information in databases by state agencies. Examples include:

RSA 189 Student and Teacher Information Protection and Privacy establishes process and procedure for the Department of Education in its collection and management of student and teacher data.

RSA 153-A:35 Emergency Medical and Trauma Services - Protected Health Information; Privacy Committee Established. The law establishes a privacy committee under the Department of Safety to review and approve requests for the use of emergency medical and trauma services records data.

RSA 437:8-a Animal Records Database Established. The law establishes an animal records database and confidentiality policies under the Department of Agriculture.

RSA 126 - 24-a. Bureau of Health Statistics and Data Management and Vital Records Privacy Board of Health-Related Research. A specific law pertaining to protected health information in accordance with the Health Insurance Portability and Accountability Act ("HIPAA").

RSA 126-A:89-97 Controlled Drug Prescription Health and Safety Program. A specific law relative to an electronic system database to facilitate confidential sharing of information related to the prescribing and dispensing of controlled substances.

Other State laws. According to source OneTrust.com, a technology company that works to define platforms for privacy, security, and trust, only a couple of states in the United States have comprehensive privacy laws, namely California, Virginia and Colorado. While the focus of this Committee is specific to the closed loop referral system, looking at how other states are addressing personal privacy is educational. State laws in California and Virginia, for example, define what personal data is and how to define a consumer. The laws go on to further define consumer rights, including Opt-in/Opt-out rights, rights to delete information and rights to data portability. Policies also include requirements for uniform consent and enforcement mechanisms for violations and/or breaches of personal privacy.

IV. Privacy Impact Assessment RMP Example

A. Executive Summary

This Privacy Impact Assessment has been conducted in accordance with the [COMPANY] Privacy Policy, which can be found at: <include link to Policy>. The privacy-related risks or control deficiencies identified in this *Risk Summary & Mitigation Plan* have been evaluated based on the comprehensive requirements stemming from the [COMPANY] Privacy Policy, and other applicable [COMPANY] policies, SOPs, or control requirements.

A.1. Description of the Processing Activity

Purpose for Processing Personal or Sensitive Personal Information	*Provide the purpose for Processing the Personal Information in plain language such that it may be easily understood by those not necessarily familiar with the Processing Activity* *Include a reference to applicable a "legitimate purpose" as set forth in the [COMPANY] Privacy Policy.*
Process Description	*Provide a brief description of the Processing Activity with a focus on the aspects related to Personal* Information. *The objective is to provide a description that would be easily understood by someone f rom outside the function / organization (avoid internal acronyms, terms of art, and other language not likely understood outside of [COMPANY]).*
Categories Data Subjects	*<e.g., Patients, HCPs, Employees, Caregivers>*
Personal Data Attributes	*<describe briefly and/or refer to section further in document where the elements are listed or described in detail>*
Location of Data Subjects	*<provide list of US states, countries, or regions if applicable. Note, if Data Subject origin spans the US, or is likely to, simply indicate "US." This is aimed at ensuring any applicable state law requirements are addressed appropriately>* ***This field may be populated (c/p) from the PA Intake Questionnaire**.*
Location of Processing (by [COMPANY])	*<list primary Processing locations, i.e., where [COMPANY] data (Personal Information) is managed>* • *STATE, COUNTRY* • *STATE, COUNTRY*
Third Parties (non-[COMPANY]) involved in Processing Activity, or engaged specifically to Process Personal Information for [COMPANY]	*<provide list of Third Parties involved in Processing (collection, hosting, providing services, or performing other actions under the engagement that would either allow access to or Processing of Personal Information subject to the Processing Activity>* ***This field may be populated (c/p) from the PA Intake Questionnaire**.*
Systems ([COMPANY]) / processes related to data processing activities (including collection/distribution)	*<provide list of applicable systems managed by [COMPANY] or third parties, as applicable – e.g., systems used to collect, manage, transfer, store or otherwise Process Personal Information subject to the Processing Activity>* • *system name* • *system name* • *system name*

A.2. Other Relevant Characteristics

<This section should include any other relevant characteristics of significance that should be understood by the Responsible Executive / PRIVACY OFFICER and that may be relevant to residual risks associated with the Processing Activity. If nothing of significance is identified, remove this entire section or state "None.">

A.3. Statement of Residual Risk

<This section should contain a summary statement regarding the "residual risks" associated with the Processing Activity.>

The objective of this section is to fully inform the [Business Executive or designee] of their accountability for any residual risks associated with the Processing Activity as well as their responsibilities under the [COMPANY] Privacy Policy. The "Sign -off" portion of this Risk Summary & Mitigation Plan is intended to document the organization's (through the Business Executive or designee):

- *Commitment to the actions (mitigations) as outlined in the Mitigation Plan*
- *Clear understanding of any remaining risks to [COMPANY] and to the impacted data subjects, as well as an appreciation that any Processing of Personal Information involves some level of (inherent) risk, not all of which can be definitively identified (future, unknown, etc.) or fully mitigated in all situations.*
- *Understanding that where accepted risks are perceived by the subject matter experts (Privacy Officer or those performing the PIA) to be disproportionate to the Processing Activities or may have potentially significant impact(s) on [COMPANY], escalation to Executive Management via the Privacy Officer, may be warranted.*

Elements to include in the Statement of Residual Risk:

- ***What risk(s) to Data Subjects and to [COMPANY], does the current the Processing Activity cause or might it result in?***
- ***What (major) findings (from the PIA) contribute to that risk?***
- ***What is the risk if the proposed mitigations are (all / partly / some) are implemented?***

Additional Drafting Guidance:

- *Assume that the audience (executing the sign-off) can find detailed information in the remaining body of the document. This section should include only a very high-level summary, to avoid redundancy.*
- *Be concise and to the point.*
- *Describe the core Processing of Personal Information intended and what the (also, very high level) risks of proceeding as planned may be, as well as what incremental requirements may exist for higher-risk activities.*
- *Describe any key gaps or deficiencies, if any.*
- *Describe what should be done to address the findings and mitigate (decrease) risk before initiating or continuing the Processing Activity.*
- *Indicate what impact, if any, delays in mitigation implementation may have, or where such delays may be acceptable, and for how long after commencement of the Processing Activity.*
- *Describe what the business is agreeing to mitigate (or what mitigations are being rejected), and any residual risks that may exist after mitigations are implemented (or rejected).*
- *Identify the need for escalation depending on the potential impact of the risks, or if agreement as to appropriate / acceptable mitigations cannot be reached.*

A.4. Review/Update Triggers

This Privacy Impact Assessment (PIA) must be reviewed and updated as necessary prior to any of the following:

1. *<list review/update triggers, e.g., expansion of countries from which Personal Information is collected, Processed, stored etc., change of third-party data processors, extend this list as necessary>*
2. New Processing of any additional Personal or Sensitive Personal Information (additional data elements), other than those reviewed in this assessment.
3. Upon expiration of next review date as indicated above.
4. Where deemed necessary by the Privacy Officer.

B. Processing Activity & Overview

B.1. Introduction

A Privacy Impact Assessment (PIA) for the <*name of the Processing Activity*> was conducted *<date or other time-period specification>* by *<Data Privacy Champion name and position>*. This assessment was based on *<describe how information relevant to the Processing Activity was obtained, e.g., "interviews conducted with <named [COMPANY] Personnel>, information provided by <Name [COMPANY] Personnel>, information provided by <third-party providers, if applicable>, etc.".*

B.2. Description

Provide a generic/basic description of the Processing Activity, including, for example:

- *a visual (data flow diagram, flow chart and/or any other conceptual diagram) of the process that illustrates the textual description as in the items below:*
- *how Personal Information is obtained, used and finally disposed of, and by whom and where etc.*
- *the type of process, activity or application, e.g., server/client, web-based etc.*
- *data controller/processor roles, if applicable*
- *origin of Personal Information, location of data systems and storage etc.*
- *overview of data protection measures in place (security)*
- *status of the Processing Activity – e.g., in use, in development, to be extended etc.*
- *the involvement of third parties and their role(s) in the process, etc.*

This is a key section of the RMP as it is intended to document and explain essential elements of the Processing Activity to those who may be unfamiliar with the context. The text should clearly describe the basis for any findings and mitigations (for example, if a subsequent / successor Data Privacy Champion, other [COMPANY] Stakeholder were to step into the role, or, if required, in response to a regulator inquiry regarding the Processing Activity).
This section should be considered a summary of the "research" performed by the individual(s) conducting the Privacy Impact Assessment. In some instances, it may be necessary to include cross-references to other documentation related to the Processing Activity (e.g., third-party service provider agreements, documented security controls, etc.). However, the aim is to include sufficient detail in this document to provide a clear picture of the relevant Processing Activity, the privacy impact (to Data Subjects), privacy-related risks / gaps, and mitigations proposed / implemented, allowing this document to serve as a stand-alone memorialization of the PIA process.
The length of the section will correspond to the complexity of the subject and/or the risks involved.

B.3. Personal Information

"Personal Information", and "Sensitive Personal Information" are defined in the POLICY LINK. The *<name of the Process, Application, Database or Initiative>* envisions the Processing of *<or Processes, if currently active>* Personal Information *<and Sensitive Personal Information, if applicable>*, of *<add as applicable: Employees, Customers, Patients, Providers, and Physicians. Include an indication of the volume of data subjects for each category (**NOTE:** this information should align with and may be taken directly from the Processing Activity Intake Questionnaire.)>*
<For each data type/category that will be Processed, include a table (example below). This could be separate tables for e.g. , customer data, web site user data, patient data, physician contact data etc.>
***NOTE**: Remember to include information that may be accessed or accessible by IT (internal or third-party IT service providers) support personnel, application developers (for maintenance & bug fixing), etc.*

B.3.1. *< Patient Data>*

The following Personal / Sensitive Personal Information are collected by *<specify who collects> <when & how>* from *<include category of data subjects, e.g., patients, employees, etc.>* and stored *<storage location>* for *<period of storage>.*
*<Provide a list or table identifying the Personal Information elements (**see example**, below) to be processed in the context of the Processing Activity>*

First name	*Work phone*	*Therapy data*
Middle name	*Alternate phone*	*Primary care physician*
Last name	*Fax*	*Specialty physician*
Address	*Email*	*Clinician*
City	*Gender*	*Primary and secondary insurance provider*

State	*Marital status*	*Primary and secondary insurance number*
Postal code	*Birth date*	*Primary and secondary group number*
Country	*Photograph*	*Primary and secondary policy holder name*
Home phone	*Prescription data*	*Primary and secondary policy relationship*

<Alternatively, if not obvious, or if warranted for clarity, provide relevant information regarding each element of Personal Information attribute>

Data field:	**Comments:**
Employee number	*<used to e.g., link to salary information system>*
Name and address	*<used to send reports, web shop offers, birthday congratulations >*
Birthdate	*<used to send employee birthday messages>*

C. Findings

Based on the information provided, the following privacy risks and control deficiencies have been identified with respect to the Processing of Personal Information in the context of *<name of the Processing Activity>*. Risks and deficiencies have been documented as findings, which are identified as follows (in order of significance):

1. ***<Textual summary of finding one>***
   <detailed description>
2. **<Textual summary of finding two>**
   <detailed description>
   . . . <include additional findings as needed>

<Note: common findings may include, for example: a) Undefined data retention time-frame policy exists; b) Insufficient security controls c) Insufficient notice provided to individuals upon collection of Personal Information; d) No Third-Party Agreement with Personal Information Protection language identified>

The following section contains the Mitigation Plan, which further details the above Findings and Risks and proposed mitigations to enable the *<name of the Processing Activity>* to proceed in compliance with the [COMPANY] Privacy Policy.
Additional findings and mitigations may be identified upon review of any additional information provided to the *<applicable [COMPANY] Privacy Officer / Representative>.* The Business (Executive and appointed action owners) is responsible for implementing and managing these mitigations appropriately, and reporting mitigation implementation status, as agreed, below.

D. Mitigation Plan

D.1. Finding & Proposed Mitigations Table

Finding	**Deficiency / Risk**	**Recommended Remediation & Mitigation Actions**	**Status**
1	*<Statement of risk(s) related to the finding>*	*<Description of remediation/mitigation actions>* *<Where applicable and possible, provide references to the [COMPANY] Privacy Policy. Referencing applicable policies will help to address questions regarding requirements (i.e., the "who says I gotta"-type pushback)>*	**Owner:** *<name>* **Due Date:** *<date>* **Verified By:** *<name>*
2		References:	**Owner:** *<name>* **Due Date:** *<date>* **Verified By:** *<name>*
3		References:	**Owner:** *<name>* **Due Date:** *<date>* **Verified By:** *<name>*

Finding	Deficiency / Risk	Recommended Remediation & Mitigation Actions	Status
5		References:	**Owner:** *<name>* **Due Date:** *<date>* **Verified By:** *<name>*
6		References:	**Owner:** *<name>* **Due Date:** *<date>* **Verified By:** *<name>*

D.2. Mitigation Status Reporting

Mitigation implementation status shall be reported by *<respective action owner>* to the applicable Privacy Officer (or other designated representative) on a *<weekly, bi-weekly, monthly, etc.>* basis until all agreed-to mitigations are implemented.

V. Unite Us Consent Form

Found on HHS Oversight Webpage:

"Closed Loop Referral Process - Attachment B Consent and Privacy Notice 2020"
http://gencourt.state.nh.us/statstudcomm/committees/72/documents/Closed%20Loop%20Referral%20Process%20-%20Attachment%20B%20Consent%20and%20Privacy%20Notice%202020%20(4%20pages).pdf

VI. Privacy Impact Assessment Executive Summary Closed Loop Referral System by DHHS.

Executive Summary

I. Background

Federal and State governments recognize both the advantages and risks of using information technology (IT) to serve the public. Members of the public and private-sector organizations interacting with the Federal and State Governments must be assured that their sensitive personal information is protected. In order to protect the privacy of individuals' personal information held by State and Federal Government agencies, compliance with requirements established by state and federal laws, regulations, and Executive Orders are enforced. Federal laws relating to safeguarding individual data in systems of records include the Privacy Act, E-Government Act of 2002 and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) agencies. One of the key tools for managing privacy risk is the Privacy Impact Assessment (PIA).

While the State of New Hampshire is only required to comply with the laws and requirements applicable for its use of health care related, personal information and federally regulated data, the Department is responsible to ensure its contractors have established, and are maintaining, appropriate administrative, technical, and physical safeguards to protect the confidentiality of the data and to prevent unauthorized use or access to it.

The purpose of the Closed Loop Referral System (CLRS), currently hosted for the State of New Hampshire by Unite USA Inc. (Unite Us), is to establish a network of participating providers (Network Participants) and facilitate the connection of an individual seeking services with an appropriate provider in or close to the individual's community. The Network serves individuals seeking services to address their social and clinical needs with the goal of positively impacting the individual's overall health outcome(s). The CLRS is designed to facilitate referrals, care coordination, and case management for services to individuals who face obstacles seeking and receiving the aforementioned independently. Examples of the type of referrals made include: organizations offering health care, treatment, food, housing, domestic violence support or legal support. The CLRS includes substance use disorder (SUD) services designated as "sensitive" and is designed to maintain the confidentiality and information security safeguards required for use and disclosure of protected health information, personally identifiable information, and legal matters as required by law for all services and individuals.

II. PIA Purpose and Scope

Purpose

The purpose of conducting a Privacy Impact Assessment (PIA) is to assess the system to identify the existence of any privacy or security risks to the information, to determine if appropriate privacy and information security safeguards are in place and to mitigate those risks to ensure the proper use and protection of the client information.

Scope

The PIA covers the type of information stored in the CLRS, how the data is collected, used and transmitted; and who is permitted access to see and use the data. Consideration was also given to the provisions of the Unite Us, client consent, privacy notice, end user and network participant agreements, and its security and privacy requirements and policies. The data within the system consists of protected health information (PHI), personally identifiable information (PII), substance use disorder (SUD) information, insurance information and other information called "sensitive information" such as legal service information, and Network Participant service provider information. Users of the Unite Us Platform consist of Network Participants (service providers) and authorized Unite Us, System Administrators (SA), support and technical staff (end users).

III. PIA Approach

A questionnaire and hypothetical case scenarios were developed in accordance with the FIPS 199- Standards for Security Categorization of Federal Information and Information Systems, Office of Management and Budget (OMB) requirements, The Privacy Act of 1974, The National Institute of Standard and Technology (NIST) recommendations, and the Federal Enterprise Architecture Business Reference Model (BRM). The questionnaire was developed in order to identify potential privacy vulnerabilities to client data or to client privacy rights.

The questionnaire was given to Unite US the vendor contracted by the Department to host the NH CLRS for its response. The Department's Privacy Officer and Deputy Information Security Officer (DISO) under the direction of the Director of the Department's Business Information Systems (BIS) corresponded and spoke with privacy, IT and security professionals of Unite Us to discuss the concerns and responses to privacy and technology questions posed in the questionnaire, hypothetical case scenarios and Unite Us stated privacy and security controls. Responses from the Unite Us, Information Security Officer (ISO) and the SME's of Unite Us were obtained and used as the basis for the PIA.

IV. System Characterization

All communication between the Unite Us staff and Network Participants occurs over the CLRS platform. The CLRS is a stand-alone system and is not connected to or integrated with the Network Participant systems. All information is either uploaded into the system or inputted manually by end users.

V. PIA Results and Mitigation Strategies

The PIA assessment confirmed that the CLRS contains PHI, PII, SUD and other sensitive data and that only those who are authorized to use the system have access to the information contained therein. The information collected, stored, and used by Unite Us, and the Network Participants is being used appropriately, is in compliance with state and federal law, with client consent, and is relevant to the purpose of the CLRS. Appropriate privacy controls are in place to ensure use is minimum necessary and sensitive information, such as substance use disorder (SUD) information, is appropriately masked and safeguarded with access strictly limited. Only the users explicitly authorized to use the CLRS have access to the platform.

As a result of the PIA the Department concludes that there are several areas that could benefit from enhanced awareness and transparency of the CLRS. Improved clarity surrounding the training, content, communication and documentation of the consent form, and the content of the Privacy Notice, End User and Network Participant Agreements will result in a better understanding by the individuals being served and the providers of the services. Further documentation of standards of practice are needed in the privacy and security user requirements within the end user and network participant agreements to ensure the proper use and collection of data in accordance with client consent.

A common opportunity for improvement in systems providing care coordination for individuals is the retention of information and the potential for human error in the data entry of the information. Additional periodic auditing of the data contained in the system should be added to the standards of practice to address data retention and accuracy of the data contained within the system.

While the information collected, stored and used by the CLRS is being used appropriately and in compliance with state and federal law, recommended opportunities for continued improvement include: revision of the Unite Us privacy notice and consent for clarity; revision of the Unite Us End-User and Network Participant Agreements for clarity; the creation of a written consent process and standard consent training; revision and documentation of data retention and destruction practices which align with the NH DHHS/Unite Us contract; and auditing capacity for access controls.

VI. Summary

The CLRS is administered by the Department and operated through a contracted technology platform, hosted by Unite Us;

however, the CLRS is not part of the NH DHHS or State IT systems. The CLRS collects, uses, maintains, and stores PHI, PII, SUD and other protected information about individual clients who receive services from network participants of the CLRS. As with all systems containing protected information, in the event the platform was breached or information disclosed without proper authorization individual's privacy could be placed at risk. The potential for loss could result in a disruption of services and/or identity theft, financial impact and mental health issues related to stress, due to the aforementioned data loss repercussions. The Unite Us platform operates in adherence to security and privacy laws and practices regarding the use, consent and transmittal of the data stored on the system. The recommendations found herein are opportunities to improve on the already compliant solution to increase clarity and awareness of the benefits of using the network to improve care and health outcomes for the individuals in New Hampshire.

VII. Unite USA Training document (pg 1 & pg 17 (proprietary)



