MEMORANDUM OF UNDERSTANDING
Between

San Bernardino County Department of Behavioral Health
and
Holmusk Technologies Inc.
for
mConnect – Major Depressive Disorder Digital Solution Study

March 1, 2022 through February 28, 2025

WHEREAS, San Bernardino County Department of Behavioral Health, hereinafter referred to as DBH, provides mental health services to consumers and their families in San Bernardino County; and

WHEREAS, Holmusk Technologies Inc., hereinafter referred to as Holmusk, seeks partners and providers to build solutions that improve outcomes, by leveraging advanced analytics and digital capabilities; and

WHEREAS, DBH and Holmusk desire to enter into an agreement for the purpose of providing a digital solution by collecting and combining all the key elements of data from both the Electronic Health Record (EHR) and patient-generated data and displaying relevant trends to the physician/provider and patient; and

WHEREAS, DBH will provide patient pool and allocate resources and provider time to support mConnect – Major Depressive Disorder (MDD) Digital Solution Study; and

WHEREAS, DBH desires that such a study that utilizes a digital solution be conducted and Holmusk agrees to provide this digital solution for this study, these services as set forth below;

NOW THEREFORE, DBH and Holmusk mutually agree to the following terms and conditions:

TABLE OF CONTENTS

I. PURPOSE

The California Advancing and Innovating Medi-Cal (CalAIM) wavier discussions have opened up positive trends to transform Behavioral Health Care. Partnering with Holmusk provides an innovative opportunity to utilize digital technologies to address Value-Based Care payment models' future direction. Value-based programs reward health care providers with incentive payments for the quality of care they give to people with Medicare. These programs are part of a larger quality strategy to reform how health care is delivered and paid for. A digitally powered data-driven platform will enhance DBH's efforts to move towards Value-Based Payment models that improve patients' outcomes with a Serious Mental Illness. This study will test a mobile application intended to assist doctors and patients in tracking symptoms of depression over the course of treatment. The study will last approximately six months and recruit up to 25-50 patients with MDD undergoing outpatient appointments. The study will investigate whether mConnect, a patient mobile application and clinician dashboard solution, can be easily used, is constantly accessible, and whether it will work well for MDD patients and doctors respectively. The mobile application will ask participants to complete five questionnaires either once a week or once every two weeks and will also measure participant's activity and sleep data. In addition to the use of the application, patients will attend doctor visits at least once a month until the end-of-the-study visit at Week 12. After the completion of the test period, the application will be removed from the patient's smartphone. Both patients and their doctors will be asked to provide feedback about their experience using mConnect.

The objective is to utilize a digital remote measurement of disease trajectory and outcomes and provide proactive/preemptive care and patient engagement. Initial application and pilot activity will include implementation in one (1) DBH outpatient clinic (Mariposa) for an estimated 25-50 mental health clients diagnosed with MDD.

The mConnect application will provide a client-centric solution to encourage client participation, improve the quality, personalization of care and treatment outcomes of clients with MDD by enabling measurement-based care. mConnect will integrate data from DBH's EHR (myAvatar) and client reported data through a mobile application. Implementation will provide for more efficient and effective quality reporting. This aligns DBH with CalAIM initiatives and the Centers for Medicare and Medicaid Services (CMS) value-based delivery models. The alignment also advances quality care and cost efficiency. This agreement will require data exchange directly from DBH's EHR/myAvatar system, therefore a Business Associate Agreement **Attachment I** and Data Security Requirements **Attachment II** will be necessary.

II. DEFINITIONS

A. Authorization for Release of Protected Health Information (PHI): A HIPAA compliant authorization signed by the client or client's legal representative, authorizing DBH to release the client's information to a designated recipient. This form must be completed thoroughly with specified records to be shared, a designated time frame and expiration date, as well as a signature by the DBH client or his/her legal representative. If the form

is signed by a legal representative, proof from the court system designating legal representation must accompany the request.

B. Department of Behavioral Health (DBH): The County of San Bernardino Department of Behavioral Health, under state law, provides mental health and substance use disorder treatment services to County residents. In order to maintain a continuum of care, DBH operates or contracts for the provision of prevention and early intervention services, 24-hour care, day treatment outpatient services, case management, and crisis and referral services. Community services are provided in all major County metropolitan areas and are readily accessible to County residents.

C. Health Insurance Portability and Accountability Act (HIPAA): A federal law designed to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.

D. Holmusk: Holmusk is on a mission to reinvent behavioral health and transform lives with Real-World Evidence and digital innovation. Headquartered in Singapore and New York, Holmusk generates evidence and builds digital solutions to advance behavioral health research, innovation, and care.

E. Institutional Review Board (IRB): Under United States Food and Drug Administration (FDA) regulations, an appropriately constituted group that has been formally designated to review and monitor biomedical research involving human subjects. In accordance with FDA regulations, an IRB has the authority to approve, require modifications in (to secure approval), or disapprove research.

F. mConnect: mConnect is a digital health solution for patients suffering from Major Depressive Disorder ("MDD"). mConnect functionally consists of the following components, each being a "Core Component":

- Patient-facing mobile application (App) capturing PHQ-9, WSAS, medication side-effects, medication adherence, patient mood tracking, and captures passive data from wearable devices that may be synced to third party platforms (e.g., sleep, activity).

- Clinician-facing dashboard which integrates and visualizes clinical EMR data (as available), and App data (i.e., patient-reported outcomes ("PROs"), and side-effects) to enable Measurement Based Care ("MBC") and personalized treatment of MDD patients.

- Clinical Coordinator dashboard with administrative privileges to manage clinician and patient accounts for each clinic/hospital.

G. MOU: Memorandum of Understanding is a document describing an agreement between parties.

H. Personally Identifiable Information (PII): PII is information that can be used alone or in conjunction with other personal or identifying information, which is linked or linkable to a specific individual. This includes: name, social security number, date of birth, address, driver's license, photo identification, other identifying number (case number, client index number, SIMON number/medical record number, etc.).

I. Protected Health Information (PHI): PHI is individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper or oral. Individually identifiable information is information, including demographic data, that relates to the individual's past, present or future physical or mental health or condition; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual, and identifies the individual or for which there is reasonable basis to believe it can be used to identify the individual.

III. SCOPE OF WORK

There are four phases of the Scope of Work.

Phase I - Approvals and Agreements

A. Complete and obtain approval from DBH's Institutional Review Board (IRB)

B. Execute DBH's Business Associate Agreement

C. Meet DBH's Data Security Requirements

Phase 2 - Deploy Current version of mConnect

A. Deploy current version of mConnect with the following refinements to:

1. Data management practices and activities to be in accordance with state and federal privacy laws, including HIPAA Privacy and Security Rules; Welfare and Institutions Code §5328; and 42 Code of Federal Regulations, Part 2. All requirements, including physical, technical and administrative safeguards are outlined in the Data Security Requirements (**Attachment II**).

2. mConnect database to integrate with NetSmart - The mConnect system has a database that will store the results of the information gathered. Once the pilot is evaluated and determined to be implemented fully, objective will be to have an interface established between DBH's EHR (myAvatar) and the mConnect database.

3. Accommodate data from NetSmart

4. Develop & deploy a Spanish version of patient app

B. Limited deployment to 1 clinic with a small patient cohort (n=25-50) and capture data

C. Align on Phase 3 and Phase 4 plan; initiate early Phase 3 work

Phase 3 - Deploy Current version of mConnect at all DBH operated Community Clinics

A. Complete initial limited roll-out and capture learnings

B. Conduct iterative development of mConnect – potential features include support for mental health comorbidities, enhancements for patient engagement, etc.

C. Align on additional data needed to support integrated outcomes and mechanism for linkage to mConnect database by DBH

D. Complete approvals, Business Associate Agreement and contract for roll out in up to 7 clinics

E. Deploy mConnect platform

Phase 4 - Scale-up data capture on mConnect platform and generate insights

A. Onboard up to 7 clinics onto mConnect platform and capture data

B. Assess relationship between treatment, outcome measures and cost; develop predictive models

C. Identify potential leading indicators of poor outcomes and high costs

D. Assess learning from roll out to refine mConnect platform

E. Determine path to establish strength of relationships in analysis and expand across behavioral health

IV. GUIDING PRINCIPLES

As a pilot study, the study will focus on beta-testing mConnect, the study will not assess efficacy or patient outcomes. This is not a clinical trial. The goal of the study is to assess feasibility and acceptability of a digital app and a clinician dashboard as a mechanism for facilitating Measurement Based Care. The study seeks to establish the feasibility of the digital solution for MDD (mConnect) on a pool of outpatients. Using the combination of patients' clinical assessment and other information (e.g., prescriptions) in the EHR and patients' active and passive data through the mobile application, the study will be assessed by the following criteria:

- Whether the integrated digital solution works and has full availability at the 99th percentile, while maintaining data privacy, consistency, and integrity; and
- Feedback provided from clinicians and patients in their reviews of mConnect clinician dashboard and patient mobile application respectively.

As a pilot study, the study will not assess efficacy and improved outcomes of patients arising from the use of the digital solution. This is a single site proof of concept study.

The project will improve provider/patient engagement through an interactive patient portal. Most EHR patient portals do not equal patient engagement. EHR's patient portals are limited to providing visit records, alerts, and secured email communication available to patients. Holmusk patient portal enables a direct and interactive exchange with patients, ensuring progress against care plans with consistent, real-time access to address emergent symptoms and transitions in care. Patient-provider interaction will increase through the use of the mConnect technology. The data on the dashboard will prompt the patient and provider to interact on patient progress and allow the provider to provide positive feedback and encouragement.

The project will provide real-time or frequent patient data on symptoms and functioning. Current reliance is on lagging outcome measures or encounters of critical events. The project allows for an opportunity for the provider to intervene upstream or proactively by providing feedback on medication monitoring, symptoms management, and progression towards treatment goals. mConnect will not be used to diagnose patients or provide any treatment recommendations.

The project provides the opportunity for providers to analyze patient data to uncover safety issues, manage clinical risk, and identify any unusual or adverse reactions to medications and treatments. Providers can obtain current information recorded in the here and now rather than relying on historical self-reports that are often unreliable. The project will allow DBH providers to move from reactive treatment planning to proactive treatment planning. Proactive treatment planning will enhance evidence-based care treatment by minimizing adverse events that have the most significant negative impact on patients' well-being and program cost - for example, unnecessary emergency visits and avoidable inpatient hospitalization.

The project will provide patients a more active part in their care and treatment by engaging them in active monitoring of symptoms. Self-monitoring is an essential clinical technique used in

cognitive-behavioral therapy, and studies have shown a significant Behavioral Modification effect.

The project will allow DBH to move from quantity data measurements to quality data measurements required in Value-Based payment models. It will provide an opportunity to design, implement, and research quality-based behavioral health metrics and outcomes not obtainable in DBH's current EHR.

The study will last approximately six months with each study participant followed for about 12 weeks. As part of routine standard of care, clinicians will see the study participants at least once a month during the period of the study. The interval between visits and number of visits during the 12 weeks period will be decided by the clinician depending on their condition.

V. ROLES AND RESPONSIBILITIES

DBH

- DBH will assign a lead Principal Investigator (PI) as study coordinator.
- DBH will assign a project manager to manage administrative and data collection activities.
- DBH will review and approve IRB application including:
  - Study Informed consent document for DBH participants.
  - The participating DBH population/sites.
  - The data elements that will be requested from DBH.
- DBH will Identify patients with a Major Depressive Disorder for the project/study's Population.
- Substance Use Disorders (SUD) are commonly an exclusion criterion, but patients with an identified SUD will likely be included due to DBH patient population.
- DBH will conduct the American Society of Addiction Medicine assessment (ASAM) evaluation for all study participants to assess the presence/severity of SUD and determine if they should participate in the study.
- DBH PI provides input on the inclusion/exclusion criteria related to ASAM.
- DBH will administer The Patient Health Questionnaire **(**PHQ**)-**9, the MDD module of the full PHQ on all study participants.
- The DBH provider will see the patient either at the outpatient clinics or via telehealth consultations per standard of care.

Holmusk:

- Complete DBH IRB application for review and approval, including:
  - Study Informed consent document for DBH participants.
  - The participating DBH population/sites.
  - The data elements that will be requested from DBH.
- Coordinate meetings between DBH, mConnect study team, and PI.

- Set up recurring meetings with select DBH team members once PI and/or point of contact is identified to refine and finalize protocol.
- Deploy a current version of mConnect with the following refinements to:
  - Spanish language version
- Will accommodate data from DBH EHR.
- Will comply with CA and SBDBH data security/privacy requirements.
  - Complete DBH Business Associate Agreement (see Attachment I)
  - Complete DBH Data Security Requirements (see Attachment II)

Mutual:

- DBH and Holmusk will mutually coordinate efforts documented in the approved IRB.
  - For the Study design and Study procedures:
    - Define Study Population and Number of patients to be enrolled
    - Inclusion / Exclusion Criteria
    - Screening and Recruitment and onboarding process
    - Patient active and passive reported data
    - Provider Visits
    - End of Study Visit
    - Withdrawal and Dropout
  - Data Analysis
    - Data Collection and Quality Assurance
    - Electronic Health Record Integration
    - Patient Mobile Application
    - Clinician Dashboard
    - Data Storage
  - Sample Size and Statistical Methods
    - Determination of Sample Size
    - Outcome Measurement Analysis
  - Ethical Considerations
    - Informed Consent
    - IRB Review
    - Confidentiality of Data

For additional details about responsibilities see **Attachment III** – IRB Application Forms. The IRB Application provides all details of the pilot study that were reviewed and approved by the IRB.

VI. FISCAL PROVISIONS

No financial commitment is to be applied between parties. Each party will be responsible for their own expenses in executing the terms of this agreement.

VII. RIGHT TO MONITOR AND AUDIT

A. DBH staff or any subdivision or appointee thereof, and the State of California or any subdivision or appointee thereof, including the Inspector General, shall have the right to

review and audit all records, books, papers and documents necessary to ensure Holmusk ’s compliance with this MOU.

B. Holmuskshall cooperate with DBH in the implementation, monitoring, and evaluation of this MOU and comply with any and all reporting requirements established by this MOU.

C. All records pertaining to Section VII(A) above shall be available for examination and audit by DBH Fiscal Services staff for DBH, Federal and State representatives for a period of three years after all pending County, State and Federal audits are completed. Records of Holmusk which do not pertain to the services under this MOU shall not be subject to review or audit unless otherwise provided in this MOU.

D. Holmuskshall provide all reasonable facilities and assistance for the safety and convenience of DBH*’s* representative in the performance of their duties under this Section. All inspections and evaluations shall be performed in such a manner as will not unduly delay the work of Holmusk.

VIII. TERM

This Memorandum of Understanding (MOU) is effective as of March 1, 2022, and expires February 28, 2025, but may be terminated earlier in accordance with provisions of Section IX of this MOU. This MOU may be extended for two additional one-year periods upon written agreement of both parties, unless terminated earlier under the provisions of Section IX.

IX. EARLY TERMINATION

A. This MOU may be terminated without cause upon thirty (30) days written notice by either party. The DBH Director is authorized to exercise DBH’s rights with respect to any termination of this MOU. Holmusk, or his/her appointed designee, has authority to terminate this MOU on behalf of Holmusk .

B. If during the term of this MOU, State and/or Federal funds appropriated for the purposes of this MOU are reduced or eliminated, DBH may immediately terminate this MOU upon written notice to Holmusk .

XI. INDEMNIFICATION AND INSURANCE

A. Indemnification

Holmusk agrees to indemnify, defend (with counsel reasonably approved by the County) and hold harmless the County and its authorized officers, employees, agents and volunteers from any and all claims, actions, losses, damages, and/or liability arising out ofHolmusk ’s negligent acts or willful misconduct, including such acts, errors or omissions of any person within Holmusk ’s control and for any costs or expenses incurred by the County on account of any such claim except where such indemnification is prohibited by law.

B. Additional Insured

All policies, except for the Workers' Compensation, Errors and Omissions and Professional Liability policies shall contain endorsements naming the County and its

officers, employees, agents and volunteers as additional insured with respect to liabilities arising out of the performance of services hereunder. The additional insured endorsements shall not limit the scope of coverage for the County to vicarious liability but shall allow coverage for the County to the full extent provided by the policy. Such additional insured coverage shall be at least as broad as Additional Insured (Form B) endorsement form ISO, CG 2010.11 85.

C. Waiver of Subrogation Rights

Holmusk shall require the carriers of required coverages to waive all rights of subrogation against the County, its officers, employees, agents, volunteers, contractors, and subcontractors. All general or auto liability insurance coverage provided shall not prohibit Holmusk and Holmusk 's employees or agents from waiving the right of subrogation prior to a loss or claim. Holmusk hereby waives all rights of subrogation against the County.

D. Policies Primary and Non-Contributory

All policies required herein are to be primary and non-contributory with any insurance or self-insurance programs carried or administered by the County.

E. Severability of Interests

Holmusk agrees to ensure that coverage provided to meet these requirements is applicable separately to each insured and there will be no cross liability exclusions that preclude coverage for suits between Holmusk and the County or between the County and any other insured or additional insured under the policy.

F. Proof of Coverage

Holmusk shall furnish Certificates of Insurance to the County Department administering the MOU evidencing the insurance coverage at the time the MOU is executed. Additional endorsements, as required, shall be provided prior to the commencement of performance of services hereunder, which certificates shall provide that such insurance shall not be terminated or expire without thirty (30) days written notice to the Department and Holmusk shall maintain such insurance from the time Holmusk commences performance of services hereunder until the completion of such services. Within fifteen (15) days of the commencement of this MOU, Holmusk shall furnish a copy of the Declaration page for all applicable policies and will provide complete certified copies of the policies and all endorsements immediately upon request.

G. Acceptability of Insurance Carrier

Unless otherwise approved by Risk Management, insurance shall be written by insurers authorized to do business in the State of California and with a minimum "Best" Insurance Guide rating of "A-VII".

H. Deductibles and Self-Insured Retention

Any and all deductibles or self-insured retentions in excess of $10,000 shall be declared to and approved by Risk Management.

I. Failure to Procure Coverage

In the event that any policy of insurance required under this MOU does not comply with the requirements, is not procured, or is canceled and not replaced, the County has the right but not the obligation or duty to cancel the MOU or obtain insurance if it deems necessary and any premiums paid by the County will be promptly reimbursed by Holmusk or County payments to Holmusk will be reduced to pay for County purchased insurance.

J. Insurance Review

Insurance requirements are subject to periodic review by the County. The Director of Risk Management or designee is authorized, but not required, to reduce, waive or suspend any insurance requirements whenever Risk Management determines that any of the required insurance is not available, is unreasonably priced, or is not needed to protect the interests of the County. In addition, if the Department of Risk Management determines that heretofore unreasonably priced or unavailable types of insurance coverage or coverage limits become reasonably priced or available, the Director of Risk Management or designee is authorized, but not required, to change the above insurance requirements to require additional types of insurance coverage or higher coverage limits, provided that any such change is reasonable in light of past claims against the County, inflation, or any other item reasonably related to the County's risk.

Any change requiring additional types of insurance coverage or higher coverage limits must be made by amendment to this MOU. Holmusk agrees to execute any such amendment within thirty (30) days of receipt.

Any failure, actual or alleged, on the part of the County to monitor or enforce compliance with any of the insurance and indemnification requirements will not be deemed as a waiver of any rights on the part of the County.

K. Insurance Specifications

Holmusk agrees to provide insurance set forth in accordance with the requirements herein. If Holmusk uses existing coverage to comply with these requirements and that coverage does not meet the specified requirements, Holmusk agrees to amend, supplement or endorse the existing coverage to do so. The type(s) of insurance required is determined by the scope of the MOU services.

Without in anyway affecting the indemnity herein provided and in addition thereto, Holmusk shall secure and maintain throughout the contract term the following types of insurance with limits as shown:

1. Workers' Compensation/Employers Liability

A program of Workers' Compensation insurance or a State-approved, Self-Insurance Program in an amount and form to meet all applicable requirements of the Labor Code of the State of California, including Employer's Liability with $250,000 limits, covering all persons including volunteers providing services on behalf of Holmusk and all risks to such persons under this MOU.

If Holmusk has no employees, it may certify or warrant to the County that it does not currently have any employees or individuals who are defined as “employees” under the Labor Code and the requirement for Workers’ Compensation coverage will be waived by the County’s Director of Risk Management.

With respect to Holmusks that are non-profit corporations organized under California or Federal law, volunteers for such entities are required to be covered by Workers’ Compensation insurance.

2. Commercial/General Liability Insurance

Holmusk shall carry General Liability Insurance covering all operations performed by or on behalf of Holmusk providing coverage for bodily injury and property damage with a combined single limit of not less than one million dollars ($1,000,000), per occurrence. The policy coverage shall include:

a. Premises operations and mobile equipment.

b. Products and completed operations.

c. Broad form property damage (including completed operations).

d. Explosion, collapse and underground hazards.

e. Personal Injury.

f. Contractual liability.

g. $2,000,000 general aggregate limit.

3. Automobile Liability Insurance

Primary insurance coverage shall be written on ISO Business Auto coverage form for all owned, hired and non-owned automobiles or symbol 1 (any auto). The policy shall have a combined single limit of not less than one million dollars ($1,000,000) for bodily injury and property damage, per occurrence.

If Holmusk is transporting one or more non-employee passengers in performance of MOU services, the automobile liability policy shall have a combined single limit of two million dollars ($2,000,000) for bodily injury and property damage per occurrence.

If Holmusk owns no autos, a non-owned auto endorsement to the General Liability policy described above is acceptable.

4. Umbrella Liability Insurance

An umbrella (over primary) or excess policy may be used to comply with limits or other primary coverage requirements. When used, the umbrella policy shall apply to bodily injury/property damage, personal injury/advertising injury and shall include a "dropdown" provision providing primary coverage for any liability not covered by the primary policy. The coverage shall also apply to automobile liability.

5. Cyber Liability Insurance

Cyber Liability Insurance with limits of not less than $1,000,000 for each occurrence or event with an annual aggregate of $2,000,000 covering claims involving privacy violations, information theft, damage to or destruction of electronic information, intentional and/or unintentional release of private information, alteration of electronic information, extortion and network security. The policy shall protect the involved County entities and cover breach response cost as well as regulatory fines and penalties.

L. Professional Services Requirements

1. Professional Liability Insurance with limits of not less than one million ($1,000,000) per claim or occurrence and two million ($2,000,000) aggregate limits;

or

Errors and Omissions Liability Insurance with limits of not less than one million ($1,000,000) and two million ($2,000,000) aggregate limits;

or

Directors and Officers Insurance coverage with limits of not less than one million ($1,000,000) shall be required for contracts with charter labor committees or other not-for-profit organizations advising or acting on behalf of the County.

2. If insurance coverage is provided on a "claims made" policy, the "retroactive date" shall be shown and must be before the date of the start of the MOU work. The "claims made" insurance shall be maintained or "tail" coverage provided for a minimum of five (5) years after MOU completion.

XII. GENERAL PROVISIONS

A. No waiver of any of the provisions of the MOU documents shall be effective unless it is made in a writing which refers to provisions so waived and which is executed by the Parties. No course of dealing and no delay or failure of a Party in exercising any right under any MOU document shall affect any other or future exercise of that right or any exercise of any other right. A Party shall not be precluded from exercising a right by its having partially exercised that right or its having previously abandoned or discontinued steps to enforce that right. No course of dealing and no delay or failure of a Party in exercising any right under any MOU document shall affect any other or future exercise of that right or any exercise of any other right.

B. The Parties' actions under the MOU shall comply with all applicable laws, rules, regulations, court orders and governmental agency orders. The provisions of this MOU are specifically made severable. If a provision of the MOU is terminated or held to be invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions shall remain in full effect.

C. The venue of any action or claim brought by any Party to the MOU will be the Superior Court of California, San Bernardino County, San Bernardino District. Each Party hereby waives any law or rule of the court, which would allow them to request or demand a change of venue. If any action or claim concerning the MOU is brought by any third-party and filed in another venue, the Parties hereto agree to use their best efforts to obtain a change of venue to the Superior Court of California, San Bernardino County, San Bernardino District.

D. Any alterations, variations, modifications, or waivers of provisions of the MOU, unless specifically allowed in the MOU, shall be valid only when they have been reduced to writing, duly signed and approved by the Authorized Representatives of both parties as an amendment to this MOU. No oral understanding or agreement not incorporated herein shall be binding on any of the Parties hereto.

X. CONCLUSION

A. This MOU, consisting of sixteen (16) pages and Attachments, is the full and complete document describing services to be rendered by Holmusk to DBH, including all covenants, conditions, and benefits.

B. The signatures of the Parties affixed to this MOU affirm that they are duly authorized to commit and bind their respective departments to the terms and conditions set forth in this document.

This Agreement may be executed in any number of counterparts, each of which so executed shall be deemed to be an original, and such counterparts shall together constitute one and the same Agreement. The parties shall be entitled to sign and transmit an electronic signature of this Agreement (whether by facsimile, PDF or other email transmission), which signature shall be binding on the party whose name is contained therein. Each party providing an electronic signature agrees to promptly execute and deliver to the other party an original signed Agreement upon request.

SAN BERNARDINO COUNTY

Curt Hagman, Chairman, Board of Supervisors

Dated: _____

SIGNED AND CERTIFIED THAT A COPY OF THIS DOCUMENT HAS BEEN DELIVERED TO THE CHAIRMAN OF THE BOARD

Lynna Monell
Clerk of the Board of Supervisors
San Bernardino County

By _____
Deputy

Holmusk Technologies Inc.
(Print or type name of corporation, company, contractor, etc.)

By ► _____
(Authorized signature - sign in blue ink)

Name _____
(*Print or type name of person signing contract)*

Title _____
(Print or Type)

Dated: _____

Address _____

FOR COUNTY USE ONLY

Approved as to Legal Form	Reviewed for Contract Compliance	Reviewed/Approved by Department
►	►	►
Dawn Martin, Deputy County Counsel	Natalie Kessee, Contracts Manager	Georgina Yoshioka, Interim Director
Date _____	Date _____	Date _____

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (Agreement) supplements and is made a part of the contract (Contract) by and between the San Bernardino County Department of Behavioral Health (hereinafter Covered Entity) and Holmusk Technologies Inc. (hereinafter Business Associate). This Agreement is effective as of the effective date of the Contract.

RECITALS

WHEREAS, Covered Entity (CE) wishes to disclose certain information to Business Associate (BA) pursuant to the terms of the Contract, which may include Protected Health Information (PHI); and

WHEREAS, CE and BA intend to protect the privacy and provide for the security of the PHI disclosed to BA pursuant to the Contract in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (HITECH Act), their implementing regulations, and other applicable laws; and

WHEREAS, The Privacy Rule and the Security Rule require CE to enter into a contract containing specific requirements with BA prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, sections 164.314, subdivision (a), 164.502, subdivision (e), and 164.504, subdivision (e) of the Code of Federal Regulations (C.F.R.) and contained in this Agreement; and

WHEREAS, Pursuant to HIPAA and the HITECH Act, BA shall fulfill the responsibilities of this Agreement by being in compliance with the applicable provisions of the HIPAA Standards for Privacy of PHI set forth at 45 C.F.R. sections 164.308 (Administrative Safeguards), 164.310 (Physical Safeguards), 164.312 (Technical Safeguards), 164.316 (Policies and Procedures and Documentation Requirements), and, 164.400, et seq. and 42 United States Code (U.S.C.) section 17932 (Breach Notification Rule), in the same manner as they apply to a CE under HIPAA;

NOW THEREFORE, in consideration of the mutual promises below and the exchange of information pursuant to this Agreement, the parties agree as follows:

A. Definitions

Unless otherwise specified herein, capitalized terms used in this Agreement shall have the same meanings as given in the Privacy Rule, the Security Rule, the Breach Notification Rule, and HITECH Act, as and when amended from time to time.

1. Breach shall have the same meaning given to such term under the HIPAA Regulations [45 C.F.R. §164.402] and the HITECH Act [42 U.S.C. §§17921 et seq.], and as further described in California Civil Code section 1798.82.
2. Business Associate (BA) shall have the same meaning given to such term under the Privacy Rule, the Security Rule, and the HITECH Act, including but not limited to 42 U.S.C. section 17921 and 45 C.F.R. section 160.103.
3. Covered Entity (CE) shall have the same meaning given to such term as under the Privacy Rule and Security Rule, including, but not limited to 45 C.F.R. section 160.103.
4. Designated Record Set shall have the same meaning given to such term under 45 C.F.R. section 164.501.

5. Electronic Protected Health Information (ePHI) means PHI that is maintained in or transmitted by electronic media as defined in the Security Rule, 45 C.F.R. section 164.103.
6. Individual shall have the same meaning given to such term under 45 C.F.R. section 160.103.
7. Privacy Rule means the regulations promulgated under HIPAA by the United States Department of Health and Human Services (HHS) to protect the privacy of Protected Health Information, including, but not limited to, 45 C.F.R. Parts 160 and 164, subparts A and E.
8. Protected Health Information (PHI) shall have the same meaning given to such term under 45 C.F.R. section 160.103, limited to the information received from, or created or received by Business Associate from or on behalf of, CE.
9. Security Rule means the regulations promulgated under HIPAA by HHS to protect the security of ePHI, including, but not limited to, 45 C.F.R. Part 160 and 45 C.F.R. Part 164, subparts A and C.
10. Unsecured PHI shall have the same meaning given to such term under the HITECH Act and any guidance issued pursuant to such Act, including, but not limited to 42 U.S.C. section 17932, subdivision (h).

B. Obligations and Activities of BA

1. Permitted Uses and Disclosures

   BA may disclose PHI: (i) for the proper management and administration of BA; (ii) to carry out the legal responsibilities of BA; (iii) for purposes of Treatment, Payment and Operations (TPO); (iv) as required by law; or (v) for Data Aggregation purposes for the Health Care Operations of CE. Prior to making any other disclosures, BA must obtain a written authorization from the Individual.

   If BA discloses PHI to a third party, BA must obtain, prior to making any such disclosure, (i) reasonable written assurances from such third party that such PHI will be held confidential as provided pursuant to this Agreement and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and (ii) a written agreement from such third party to immediately notify BA of any breaches of confidentiality of the PHI, to the extent it has obtained knowledge of such breach. [42 U.S.C. section 17932; 45 C.F.R. sections 164.504(e)(2)(i), 164.504(e)(2)(i)(B), 164.504(e)(2)(ii)(A) and 164.504(e)(4)(ii)]

2. Prohibited Uses and Disclosures

   i. BA shall not use, access or further disclose PHI other than as permitted or required by this Agreement and as specified in the attached Contract or as required by law. Further, BA shall not use PHI in any manner that would constitute a violation of the Privacy Rule or the HITECH Act. BA shall disclose to its employees, subcontractors, agents, or other third parties, and request from CE, only the minimum PHI necessary to perform or fulfill a specific function required or permitted hereunder.

   ii. BA shall not use or disclose PHI for fundraising or marketing purposes.

   iii. BA shall not disclose PHI to a health plan for payment or health care operations purposes if the patient has requested this special restriction, and has paid out of pocket in full for the health care item or service to which the PHI solely relates. (42 U.S.C. section 17935(a) and 45 C.F.R. section 164.522(a)(1)(i)(A).)

iv. BA shall not directly or indirectly receive remuneration in exchange for PHI, except with the prior written consent of CE and as permitted by the HITECH Act (42 U.S.C. section 17935(d)(2); and 45 C.F.R. section 164.508); however, this prohibition shall not affect payment by CE to BA for services provided pursuant to this Agreement.

3. Appropriate Safeguards

i. BA shall implement appropriate safeguards to prevent the unauthorized use or disclosure of PHI, including, but not limited to, administrative, physical and technical safeguards that reasonably protect the confidentiality, integrity and availability of the PHI BA creates, receives, maintains, or transmits on behalf of the CE, in accordance with 45 C.F.R. sections 164.308, 164.310, 164.312 and 164.316. [45 C.F.R. sections 164.504(e)(2)(ii)(b) and 164.308(b).]

ii. In accordance with 45 C.F.R. section 164.316, BA shall maintain reasonable and appropriate written policies and procedures for its privacy and security program in order to comply with the standards, implementation specifications, or any other requirements of the Privacy Rule and applicable provisions of the Security Rule.

iii. BA shall provide appropriate training for its workforce on the requirements of the Privacy Rule and Security Rule as those regulations affect the proper handling, use confidentiality and disclosure of the CE's PHI.

Such training will include specific guidance relating to sanctions against workforce members who fail to comply with privacy and security policies and procedures and the obligations of the BA under this Agreement.

4. Subcontractors

BA shall enter into written agreements with agents and subcontractors to whom BA provides CE's PHI that impose the same restrictions and conditions on such agents and subcontractors that apply to BA with respect to such PHI, and that require compliance with all appropriate safeguards as found in this Agreement.

5. Reporting of Improper Access, Use or Disclosure or Breach

Every suspected and actual Breach shall be reported immediately, but no later than one (1) business day upon discovery, to CE's Office of Compliance, consistent with the regulations under HITECH Act. Upon discovery of a Breach or suspected Breach, BA shall complete the following actions:

i. Provide CE's Office of Compliance with the following information to include but not limited to:

a) Date the Breach or suspected Breach occurred;

b) Date the Breach or suspected Breach was discovered;

c) Number of staff, employees, subcontractors, agents or other third parties and the names and titles of each person allegedly involved;

d) Number of potentially affected Individual(s) with contact information; and

e) Description of how the Breach or suspected Breach allegedly occurred.

ii. Conduct and document a risk assessment by investigating without unreasonable delay and in no case later than five (5) calendar days of discovery of the Breach or suspected Breach to determine the following:

a) The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification;

b) The unauthorized person who had access to the PHI;

c) Whether the PHI was actually acquired or viewed; and

d) The extent to which the risk to PHI has been mitigated.

iii. Provide a completed risk assessment and investigation documentation to CE's Office of Compliance within ten (10) calendar days of discovery of the Breach or suspected Breach with a determination as to whether a Breach has occurred. At the discretion of CE, additional information may be requested.

a) If BA and CE agree that a Breach has not occurred, notification to Individual(s) is not required.

b) If a Breach has occurred, notification to the Individual(s) is required and BA must provide CE with affected Individual(s) name and contact information so that CE can provide notification.

iv. Make available to CE and governing State and Federal agencies in a time and manner designated by CE or governing State and Federal agencies, any policies, procedures, internal practices and records relating to a Breach or suspected Breach for the purposes of audit or should the CE reserve the right to conduct its own investigation and analysis.

6. Access to PHI

To the extent BA maintains a Designated Record Set on behalf of CE, BA shall make PHI maintained by BA or its agents or subcontractors in Designated Record Sets available to CE for inspection and copying within ten (10) days of a request by CE to enable CE to fulfill its obligations under the Privacy Rule. If BA maintains ePHI, BA shall provide such information in electronic format to enable CE to fulfill its obligations under the HITECH Act. If BA receives a request from an Individual for access to PHI, BA shall immediately forward such request to CE.

7. Amendment of PHI

If BA maintains a Designated Record Set on behalf of the CE, BA shall make any amendment(s) to PHI in a Designated Record Set that the CE directs or agrees to, pursuant to 45 C.F.R. section 164.526, or take other measures as necessary to satisfy CE's obligations under 45 C.F.R. section 164.526, in the time and manner designated by the CE.

8. Access to Records

BA shall make internal practices, books, and records, including policies and procedures, relating to the use, access and disclosure of PHI received from, or created or received by BA on behalf of, CE available to the Secretary of HHS, in a time and manner designated by the Secretary, for purposes of the Secretary determining CE's compliance with the Privacy Rule and Security Rule and patient confidentiality regulations. Any documentation provided to the Secretary shall also be provided to the CE upon request.

9. Accounting for Disclosures

BA, its agents and subcontractors shall document disclosures of PHI and information related to such disclosures as required by HIPAA. This requirement does not apply to disclosures made for purposes of TPO. BA shall provide an accounting of disclosures

to CE or an Individual, in the time and manner designated by the CE. BA agrees to implement a process that allows for an accounting to be collected and maintained by BA and its agents or subcontractors for at least six (6) years prior to the request. At a minimum, the information collected and maintained shall include: (i) the date of disclosure; (ii) the name of the entity or person who received PHI and, if known, the address of the entity or person; (iii) a brief description of PHI disclosed; and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the Individual's authorization, or a copy of the written request for disclosure.

10. Termination

    CE may immediately terminate this agreement, and any related agreements, if CE determines that BA has breached a material term of this agreement. CE may, at its sole discretion, provide BA an opportunity to cure the breach or end the violation within the time specified by the CE.

11. Return of PHI

    Upon termination of this Agreement, BA shall return all PHI required to be retained by the BA or its subcontractors, employees or agents on behalf of the CE. In the event the BA determines that returning the PHI is not feasible, the BA shall provide the CE with written notification of the conditions that make return not feasible. Additionally, the BA must follow established policies and procedures to ensure PHI is safeguarded and disposed of adequately in accordance with 45 C.F.R. section 164.310, and must submit to the CE a certification of destruction of PHI. For destruction of ePHI, the National Institute of Standards and Technology (NIST) guidelines must be followed. BA further agrees to extend any and all protections, limitations, and restrictions contained in this Agreement, to any PHI retained by BA or its subcontractors, employees or agents after the termination of this Agreement, and to limit any further use, access or disclosures.

12. Breach by the CE

    Pursuant to 42 U.S.C. section 17934, subdivision (b), if the BA is aware of any activity or practice by the CE that constitutes a material Breach or violation of the CE's obligations under this Agreement, the BA must take reasonable steps to address the Breach and/or end eliminate the continued violation, if the BA has the capability of mitigating said violation. If the BA is unsuccessful in eliminating the violation and the CE continues with non-compliant activity, the BA must terminate the Agreement (if feasible) and report the violation to the Secretary of HHS.

13. Mitigation

    BA shall have procedures in place to mitigate, to the extent practicable, any harmful effect that is known to BA of a use, access or disclosure of PHI by BA, its agents or subcontractors in violation of the requirements of this Agreement.

14. Costs Associated to Breach

    BA shall be responsible for reasonable costs associated with a Breach. Costs shall be based upon the required notification type as deemed appropriate and necessary by the CE and shall not be reimbursable under the Agreement at any time. CE shall determine the method to invoice the BA for said costs. Costs shall incur at the current rates and may include, but are not limited to the following:

    - Postage;

- Alternative means of notice;
- Media notification; and
- Credit monitoring services.

15. Direct Liability

    BA may be held directly liable under HIPAA for impermissible uses and disclosures of PHI; failure to provide breach notification to CE; failure to provide access to a copy of ePHI to CE or individual; failure to disclose PHI to the Secretary of HHS when investigating BA's compliance with HIPAA; failure to provide an accounting of disclosures; and, failure to enter into a business associate agreement with subcontractors.

16. Indemnification

    BA agrees to indemnify, defend and hold harmless CE and its authorized officers, employees, agents and volunteers from any and all claims, actions, losses, damages, penalties, injuries, costs and expenses (including costs for reasonable attorney fees) that are caused by or result from the acts or omissions of BA, its officers, employees, agents and subcontractors, with respect to the use, access, maintenance or disclosure of CE's PHI, including without limitation, any Breach of PHI or any expenses incurred by CE in providing required Breach notifications.

17. Judicial or Administrative Proceedings

    CE may terminate the Contract, effective immediately, if (i) BA is named as a defendant in a criminal proceeding for a violation of HIPAA, the HITECH Act, the Privacy Rule, Security Rule or other security or privacy laws or (ii) a finding or stipulation is made in any administrative or civil proceeding in which the BA has been joined that the BA has violated any standard or requirement of HIPAA, the HITECH Act, the Privacy Rule, Security Rule or other security or privacy laws.

18. Insurance

    In addition to any general and/or professional liability insurance coverage required of BA under the Contract for services, BA shall provide appropriate liability insurance coverage during the term of this Agreement to cover any and all claims, causes of action, and demands whatsoever made for loss, damage, or injury to any person arising from the breach of the security, privacy, or confidentiality obligations of BA, its agents or employees, under this Agreement and under HIPAA 45 C.F.R. Parts 160 and 164, Subparts A and E.

19. Assistance in Litigation or Administrative Proceedings

    BA shall make itself, and any subcontractors, employees, or agents assisting BA in the performance of its obligations under the Agreement, available to CE, at no cost to CE, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CE, its directors, officers, or employees based upon a claimed violation of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule, or other laws relating to security and privacy, except where BA or its subcontractor, employee or agent is a named adverse party.

C. Obligations of CE

1. CE shall notify BA of any of the following, to the extent that such may affect BA's use, access, maintenance or disclosure of PHI:

i. Any limitation(s) in CE's notice of privacy practices in accordance with 45 C.F.R. section 164.520.

ii. Any changes in, or revocation of, permission by an individual to use, access or disclose PHI.

iii. Any restriction to the use, access or disclosure of PHI that CE has agreed to in accordance with 45 C.F.R. section 164.522.

D. General Provisions

1. Remedies

BA agrees that CE shall be entitled to seek immediate injunctive relief as well as to exercise all other rights and remedies which CE may have at law or in equity in the event of an unauthorized use, access or disclosure of PHI by BA or any agent or subcontractor of BA that received PHI from BA.

2. Ownership

The PHI shall be and remain the property of the CE. BA agrees that it acquires no title or rights to the PHI.

3. Regulatory References

A reference in this Agreement to a section in the Privacy Rule and Security Rule and patient confidentiality regulations means the section as in effect or as amended.

4. No Third-Party Beneficiaries

Nothing express or implied in the Contract or this Agreement is intended to confer, nor shall anything herein confer, upon any person other than CE, BA and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

5. Amendment

The parties acknowledge that state and federal laws related to privacy and security of PHI are rapidly evolving and that amendment of the Contract or this Agreement may be required to ensure compliance with such developments. The parties shall negotiate in good faith to amend this Agreement when and as necessary to comply with applicable laws. If either party does not agree to so amend this Agreement within 30 days after receiving a request for amendment from the other, either party may terminate the Agreement upon written notice. To the extent an amendment to this Agreement is required by law and this Agreement has not been so amended to comply with the applicable law in a timely manner, the amendment required by law shall be deemed to be incorporated into this Agreement automatically and without further action required by either of the parties. Subject to the foregoing, this Agreement may not be modified, nor shall any provision hereof be waived or amended, except in a writing duly signed and agreed to by BA and CE.

6. Interpretation

Any ambiguity in this Agreement shall be resolved to permit CE to comply with the Privacy and Security Rules, the HITECH Act, and all applicable patient confidentiality regulations.

7. Compliance with State Law

In addition to HIPAA and all applicable HIPAA Regulations, BA acknowledges that BA and CE may have confidentiality and privacy obligations under State law, including, but

not limited to, the California Confidentiality of Medical Information Act (Cal. Civil Code §56, et seq. ("CMIA")). If any provisions of this Agreement or HIPAA Regulations or the HITECH Act conflict with CMIA or any other California State law regarding the degree of protection provided for PHI and patient medical records, then BA shall comply with the more restrictive requirements.

8. Survival

   The respective rights and obligations and rights of CE and BA relating to protecting the confidentiality or a patient's PHI shall survive the termination of the Contract or this Agreement.

IN WITNESS WHEREOF, the Parties have executed this Agreement to be effective as of the Effective Date.

COVERED ENTITY	**BUSINESS ASSOCIATE**
County of San Bernardino	**Entity**
Signature	**Signature**
Dated	**Dated**
Curt Hagman	
Name	**Name**
Chairman, Board of Supervisors	
Title	**Title**

DATA SECURITY REQUIREMENTS

Pursuant to its contract with the State Department of Health Care Services, the Department of Behavioral Health (DBH) requires Holmusk (Contractor) adhere to the following data security requirements:

A. Personnel Controls

1. Employee Training. All workforce members who assist in the performance of functions or activities on behalf of DBH, or access or disclose DBH Protected Health Information (PHI) or Personal Information (PI) must complete information privacy and security training, at least annually, at Contractor's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of ten (10) years from the final date of the contract period or from the date of completion of any audit, whichever is later.

2. Employee Discipline. Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.

3. Confidentiality Statement. All persons that will be working with DBH PHI or PI must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The Statement must be signed by the workforce member prior to accessing DBH PHI or PI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for DBH inspection for a period of ten (10) years from the final date of the contract period or from the date of completion of any audit, whichever is later.

4. Background Check. Before a member of the workforce may access DBH PHI or PI, a background screening of that worker must be conducted. The screening should be commensurate with the risk and magnitude of harm the employee could cause, with more thorough screening being done for those employees who are authorized to bypass significant technical and operational security controls. The Contractor shall retain each workforce member's background check documentation for a period of ten (10) years from the final date of the contract period or from the date of completion of any audit, whichever is later.

B. Technical Security Controls

1. Workstation/Laptop Encryption. All workstations and laptops that store DBH PHI or PI either directly or temporarily must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved in writing by DBH's Office of Information Technology.

2. Server Security. Servers containing unencrypted DBH PHI or PI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

3. Minimum Necessary. Only the minimum necessary amount of DBH PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.

4. Removable Media Devices. All electronic files that contain DBH PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, Blackberry, backup tapes, etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.

5. Antivirus / Malware Software. All workstations, laptops and other systems that process and/or store DBH PHI or PI must install and actively use comprehensive anti-virus software / Antimalware software solution with automatic updates scheduled at least daily.

6. Patch Management. All workstations, laptops and other systems that process and/or store DBH PHI or PI must have all critical security patches applied with system reboot if

necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within thirty (30) days of vendor release. Applications and systems that cannot be patched within this time frame due to significant operational reasons must have compensatory controls implemented to minimize risk until the patches can be installed. Application and systems that cannot be patched must have compensatory controls implemented to minimize risk, where possible.

7. User IDs and Password Controls. All users must be issued a unique user name for accessing DBH PHI or PI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed at least every ninety (90) days, preferably every sixty (60) days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:

    a. Upper case letters (A-Z)
    b. Lower case letters (a-z)
    c. Arabic numerals (0-9)
    d. Non-alphanumeric characters (special characters)

8. Data Destruction. When no longer needed, all DBH PHI or PI must be wiped using the Gutmann or U.S. Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of DBH's Office of Information Technology.

9. System Timeout. The system providing access to DBH PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than twenty (20) minutes of inactivity.

10. Warning Banners. All systems providing access to DBH PHI or PI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.

11. System Logging. The system must maintain an automated audit trail which can identify the user or system process which initiates a request for DBH PHI or PI, or which alters DBH PHI or PI. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If DBH PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least ten (10) years from the final date of the contract period or from the date of completion of any audit, whichever is later.

12. Access Controls. The system providing access to DBH PHI or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.

13. Transmission Encryption. All data transmissions of DBH PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing DBH PHI can be encrypted. This requirement pertains to any type of DBH PHI or PI in motion such as website access, file transfer, and E-Mail.

14. Intrusion Detection. All systems involved in accessing, holding, transporting, and protecting DBH PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

C. Audit Controls

1. System Security Review. Contractor must ensure audit control mechanisms that record and examine system activity are in place. All systems processing and/or storing DBH PHI or PI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.

2. Log Review. All systems processing and/or storing DBH PHI or PI must have a routine procedure in place to review system logs for unauthorized access.

3. Change Control. All systems processing and/or storing DBH PHI or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

D. Business Continuity/Disaster Recovery Controls

1. Emergency Mode Operation Plan. Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of DBH PHI or PI held in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than 24 hours.

2. Data Backup Plan. Contractor must have established documented procedures to backup DBH PHI to maintain retrievable exact copies of DBH PHI or PI. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore DBH PHI or PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of DBH data.

E. Paper Document Controls

1. Supervision of Data. DBH PHI or PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. DBH PHI or PI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

2. Escorting Visitors. Visitors to areas where DBH PHI or PI is contained shall be escorted and DBH PHI or PI shall be kept out of sight while visitors are in the area.

3. Confidential Destruction. DBH PHI or PI must be disposed of through confidential means, such as cross cut shredding and pulverizing.

4. Removal of Data. Only the minimum necessary DBH PHI or PI may be removed from the premises of Contractor except with express written permission of DBH. DBH PHI or PI shall not be considered “removed from the premises” if it is only being transported from one of Contractor’s locations to another of Contractor’s locations.

5. Faxing. Faxes containing DBH PHI or PI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.

6. Mailing. Mailings containing DBH PHI or PI shall be sealed and secured from damage or inappropriate viewing of such PHI or PI to the extent possible.

   Mailings which include 500 or more individually identifiable records of DBH PHI or PI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of DBH to use another method is obtained.

DBH RESEARCH PROPOSAL/ APPLICATION

Title of Project **mConnect – A Proof of Concept Study for an MDD Digital Solution**

Researcher **Holmusk / Scott Kollins**

TABLE OF CONTENTS

Additional Information

Department of Behavioral Health
San Bernardino County, California

Research Application Face Sheet

Leave Blank – RRC Use Only
Received: Comm. Date:
Assigned to: Response Date:

Title of Project (max of 200 characters, including spaces)
mConnect – A Proof of Concept Study for an MDD Digital Solution

(for RRC Use) Tracking #

Project Subtitle (max of 100 characters)
Study to display relevant trends of combined eHr and patient generated data to physician and patient

Applicant		**Sponsor** (e.g., graduate advisor, non-profit org, DBH, etc.)	
1. Name (last, first): Schreur, Christopher		9. Name (last, first): Kollins, Scott	
2. Current Position: Collaborator	3. Degree MD	10. Relationship to Applicant: Chief Medical Officer	
4. Department, School, or Organization: Department of Behavioral Healt		11. Department, School, or Organization: Holmusk	
5. Address: 303 E Vanderbilt Way, San Bernardino CA, 92415		12. Address: 54 Thompson street, New York NY, 10012	
6. Telephone: 909-388-0811	7. Fax	13. Telephone: 919-434-3392	14. Fax
8. Email: Christopher.Schreur@dbh.sbcounty.gov		15. Email: scott.kollins@holmusk.com	

16. Client contact? ☒ Yes ☐ No

17. Involves children? ☐ Yes ☒ No

18. General Design of Study ☐ Experimental ☐ Correlational (post-hoc) ☐ Survey ☐ Case Study

19. TYPE(S) OF DATA TO BE COLLECTED

- ☐ Archived Records (e.g., closed charts)
- ☒ Active Records (e.g., open charts)
- ☐ CSI Database Extracts
- ☐ Client Surveys or Instruments Administered by Researcher(s)
- ☒ Client Surveys or Instruments Administered by DBH Staff
- ☐ Other _____

20. DATES OF PROPOSED PROJECT PERIOD *(MM/DD/YY)*
From: 12/1/2021 To: 12/1/2022

21. DATE OF FINAL REPORT *(MM/DD/YY)*

22. ACADEMIC BASIS (if applicable)
☐ Thesis ☐ Dissertation ☐ Class Project
☒ Other _____

STATEMENT OF PROPOSAL: Concisely state both the project's broad, long-term objectives and specific aims, specifying how the project relates to the mental health field. Briefly describe the research design and methods for achieving these goals. This abstract is meant to serve as a succinct and accurate description of the proposed work, separate from supporting documentation. If the application is approved, this description, as is, will become public information. Therefore, do not include proprietary/confidential information.

THIS IS A FILLABLE-FORM DOCUMENT. PLEASE USE WORD PROCESSOR OR TYPE. DO NOT EXCEED THE SPACE PROVIDED.

The study seeks to establish the feasibility of the digital solution for Major depressive disorder MDD (mConnect) on a pool of outpatients. Using the combination of patients' clinical assessment and other information (e.g. prescriptions) in EHR and patients' active and passive data through the mobile application.

The study outcome will be feedback provided from clinicians and patients in their reviews of mConnect clinician dashboard and patient mobile application respectively. The study will also assess whether mConnect works and has availability within 30 seconds at the 99th percentile (include the explanation) while maintaining data privacy, consistency, and integrity.

As a pilot study, the study will not assess efficacy and improved outcomes of patients arising from the use of the digital solution. Other future app enhancements such as algorithms to provide MBC considerations and predictive components around future health of the patient including escalation of symptoms and risk of relapse may be explored in the future. This is a single site proof of concept study, a randomized clinical trial in a bigger patient population could be designed to test the efficacy on an enhanced solution.

Resources, Risks and Support Form

Project Title: **mConnect – A Proof of Concept Study for an MDD Digital Solution**

DBH Resources Needed (If no resources are needed, check here ☐. If additional forms are attached, check here ☒.)

Estimated DBH Staff Hours:2700 What type(s) of Staff?See Worksheet - DBH Resources BOE

Department Equipment:None

Other DBH resources: None

Estimated Client Hours:400

Assessment of Potential Risks (Check here if special forms or other attachments accompany this application. ☐)

Describe in detail any foreseeable risks to participants:

Patients may feel inconvenienced to complete the questionnaires regularly. Protected health information (PHI) deriving from the completed questionnaires and medical records will be used by the doctor during doctor visits. There is a risk that there may be a data breach, unauthorized personnel gain access to the data and hence potential loss of confidentiality

Describe how the researcher will mitigate these risks:

There are measures in place designed to protect Patient Personal Information in an effort to prevent loss, misuse, and unauthorized access, disclosure, alteration, and destruction of these Information. We provide HIPAA compliant physical, electronic, and procedural safeguards to protect Personal Information we process and maintain.

Special Considerations for Child Participants (complete this section if Box 17 on Face Sheet is checked)

Will this project involve direct contact with minors? ☐ Yes ☒ No

If "Yes", please describe in detail how parental/guardian informed consent for participation will be obtained and how the children's rights and welfare will be protected. (Check here if special consent forms or other attachments accompany this application. ☐)

Other Agency Involvement (If no other agencies are involved, please check here ☒.)

If other public or private agencies, schools, or institutions will be involved in this project, please describe the nature of their involvement and your specific relationship to that agency.

Direct DBH Involvement or Support (If there is no DBH involvement, please check here ☐.)

If this project relates to or is internally supported by DBH staff or administrators, please describe the nature and involvement of these personnel.

See Worksheet - DBH Resources BOE

Basis of Estimate for Estimated DBH Staff Hours

Name	Role	Hours	Basis of Estimate
Dr. Christopher Schreur	Principal Investigator	500	25 % FTE for 1 year = 2000 hours *25%
Prem Daniel	Study Coordinator	500	1 FTE for one year per Dr. Kelley and Dr. Schreur; But can be scaled down to say 25% with responsibilities given to others
List of Clinicians will be provided by Dr. Schreur	Mariposa Clinician	500	2 Hours once Monthly for 3 months for 50 clients = 2*3*50; 4 hours one time for 50 clients; End of study Clinician Exit Interview;
List of Clinic Support Staff / Case Manager / Peer Family Advocated will be provided by Mariposa Clinic Supervisor	Study Followup	800	2 hours onetime for 50 clients to setup and obtain consent; 1 hour every week for 12 weeks for 50 clients for weekly follow-up; 4 hours onetime for 50 clients - Client Exit Inteview and Transcription
IT Support for Data Extraction from Avatar/Order Connect, FTP	IT/R&E	300	Role and Work Effort to be estimated
IRB Approval and Compliance	IRB	100	
	Total	**2700**	

Basis of Estimate for Client Hours

Task		Hours	Basis of Estimate
Patient Informed Consent		50	Understand and sign Informed consent - one time
Install and configure APP		50	Install Mconnect App on phone; one time 1 hour per client
Install and configure Fitbit/Applewatch/Google Health integration		50	Integrate Mconnect with Passive Health data collection - Fitbit / Google Health; one time 1 hour per client
Weekly update of PSQ-9, WAS and other instruments and transmist		150	15 minutes per week for 12 weeks for 50 clients
Exit Interview		100	one time 2 hours per client
	Total	**400**	

List of DBH Staff Involved in the Study:		
Name	**Role**	**Nature and Involvement**
Dr. Christopher Schreur	Principal Investigator	Clinical lead responsible for overall project coordination/completion within DBH.
Prem Daniel	Study Coordinator	Project Management and Study Coordination
List of Doctor will be provided by Dr. Schreur	Mariposa Doctors	They will have access to the Clincian Dashboard to view the results of the active and passive data collected from the mobile application as part of regular outpatient treatment
List of Clinicians will be provided by Dr. Schreur and Clinic Supervisor / Program Manager	Mariposa Clinician	They will have access to the Clincian Dashboard to view the results of the active and passive data collected from the mobile application as part of regular outpatient treatment
List of Clinic Support Staff / Case Manager / PFA will be provided by Mariposa Clinic Supervisor	Study Followup	They will administer the Informed Consent from the select client, coordinate enrollment into the mConnect App and follow-up with the client once a week during the 12 week study to ensure client completed the weekly responses on the mbile app; At the end of the study, they will conduct an end of study interview with the client and transcribe the interview.
IT Support for Data Extraction from Avatar/Order Connect, FTP	IT/R&E	Select Client List for Mariposa per inclusion and Exclusion Criteria: Extract Data from Avatar and Order Connect for above clients; Demographics, Diagnosis, Medication, Claims; Provide Weekly (or more frequent) updates to data on Secure FTP to Holmusk
IRB Approval and Compliance	IRB	Review and Appprove IRB Application and Study Protocol
DBH Executive Management	Oversight	Provide Vision, Direction to DBH, Holmusk and J&J; Liaison, approval and visibility with BOE

Research & Evaluation
Department of Behavioral Health
San Bernardino County

STATEMENT OF AGREEMENT BETWEEN RESEARCH APPLICANT AND DEPARTMENT OF BEHAVIORAL HEALTH

Research applicants agree to the following conditions:

1. To conform to the ethical guidelines set forth in the APA's *Ethical Principles*, which can be obtained without cost from http://www.apa.org/ethics/code1992.html. (In June 2003, revised *Principles* will take effect; this is available at no charge at http://www.apa.org/ethics/code2002.html.
2. To immediately report any client concerns or complaints to the Department's Office of Patients' Rights, and to simultaneously inform the Chair of the Research Review Committee (RRC).
3. To immediately inform the Research Review Committee of unexpected complications that may occur during the course of the research.
4. To inform the RRC of any proposed changes in research design or methodology, and not to implement those changes without RRC approval.
5. To maintain all DBH-derived data and information in a secure and confidential manner, protecting both information that could identify clients and data that have research value.
6. To send monthly reports of the project's progress to the Department staff assigned to monitor the research, with a copy to the Chair of the Research Review Committee. (This may be done by email.)
7. To provide a copy of the project's final report, thesis or dissertation to the Research Review Committee within 60 days of project completion. In the event the project is terminated before completion, an explanatory report must be made to the Committee within 30 days of project termination.
8. To provide copies of all raw data, including data tables and spreadsheets kept in electronic format, to the Chair of the Committee, within 60 days of project completion or 30 days of termination, as applicable.
9. After conclusion or termination of the project, to securely preserve and/or destroy all DBH-derived data and information in accordance with ethical and legal guidelines.

SPECIFIC ASSURANCE OF CONFIDENTIALITY

"As a condition of doing research involving persons who have received services from the Department of Behavioral Health, San Bernardino County, California, I agree not to divulge any information obtained in the course of such research to unauthorized persons and not to publish or otherwise make public any information regarding persons who have received services in a way that the person who received services is identifiable. I understand that video and/or audio recording of clients requires special committee approval and signed consent to that effect by the client. I recognize that unauthorized release of confidential information may make me subject to civil action under provisions of California's Welfare and Institutions Code."

I agree to abide by the conditions set forth above, and understand that failure to comply may result in the termination of my project, notification of my sponsoring agency or school, and referral to ethics committees and legal authorities, as appropriate.

- -

Title of Research Proposal: **mConnect – A Proof of Concept Study for an MDD Digital Solution**

Estimated Completion Date: 12/31/2022

DocuSigned by:
Christopher Schreur
79DBECCE4C354EE...

Signature of Researcher

12/2/2021
Date

HIPAA Compliance Assurance

Project Title: **mConnect – A Proof of Concept Study for an MDD Digital Solution**

NAME OF RESPONSIBLE PERSON TO USE OR RECEIVE THE LIMITED DATA SET
LAST NAME, FIRST NAME, MIDDLE INITIAL/ORGANIZATION NAME: SUBRAMANIAM, SAI / HOLMUSK
LIST ALL OTHER PERSONS WHO WILL HAVE ACCESS TO, USE, OR DISCLOSE THE INFORMATION: *[45 C.F.R. § 164.514(e)(4)(A)(ii)(B)]* DUNAI, ANDREW

ASSURANCES
☒ The requested information and/or dataset is/are the minimum required to successfully complete this project. ☒ The use of this information presents no more than minimal risk to clients, staff or researchers. ☒ The privacy risks of this project are reasonable in relation to the anticipated benefits of the research.

DATA TO BE DISCLOSED
Clinical and claims data from NetSmart/myAvatar (see IRB Study Protocol for more details)

INTENDED USES AND DISCLOSURES OF LIMITED DATA SET
This solution will combine patients' clinical assessments during physician consultations (captured in electronic health records (EHR)) and patient generated active and passive data (collected through a mobile application called mConnect) into a proprietary data analytics engine to generate key insights for both patients and clinicians. *(The purpose is limited to research, public health or health care operations as defined by the HIPAA Privacy Rule, 45 C.F.R. § 164.501) [45 C.F.R. § 164.514(e)(4)(ii)(A)]*

SPECIFIC PLAN TO PROTECT DATA SET DURING TERM OF PROJECT
Data collected from the application will be stored in a secure cloud AWS server at the North Virginia region. Once the study is closed, an anonymized version of the dataset will be made available to Holmusk (Appendix D). This will be retained until acceptance of the final publication of data from the study. All the data is encrypted in both rest and during transit. The patient reported outcomes can only be viewed by the patient, clinician, and other authorized study team members. The clinician dashboard can only be accessed by clinicians and other authorized study team members. The access is restricted to the personnel's password protected accounts. As a general rule, the patients' personal information will be removed of identifiers when viewed by the Sponsor. Only employees, service providers and subcontractors who need the Personal Information to perform a specific job are granted access to Personal Information. Such personnel include but are not limited to Clinical Research Monitors and technical support personnel in order to troubleshoot issues patients may have with the site, the platform or accounts. If the patient data are used for any future research, only patients' non-identifiable anonymous data will be used.

SPECIFIC PLAN TO DESTROY OR RETURN DATA SET AT CONCLUSION OF PROJECT
Once the study is closed, an anonymized version of the dataset will be made available to Holmusk (Appendix D). This will be retained until acceptance of the final publication of data from the study. All the data is encrypted in both rest and during transit.

AGREEMENT
In exchange for access to the limited data set, I agree to the following: • I, *and those listed above* will not use or further disclose the information accessed or received other than as permitted by this data use agreement or as otherwise required by law. *[45 C.F.R. § 164.514(e)(4)(ii)(c)(1)]* • I, *and those listed above* will use appropriate safeguards to prevent the use or disclosure of the information other than as provided for by the data use agreement. *[45 C.F.R. § 164.514(e)(4)(ii)(c)(2)]*

- I, *and those listed above* will report to DBH any use or disclosure of the information not provided for by this data use agreement of which I, *or those listed above* become aware. *[45 C.F.R. § 164.514(e)(4)(ii)(c)(3)]*
- I, *and those listed above* ensure that any agents, including a subcontractor, to whom I, *or those listed above* provide the limited data set agree to the same restrictions and conditions that apply to myself, *or those listed above* in this agreement with respect to such information. *[45 C.F.R. § 164.514(e)(4)(ii)(c)(4)]*
- I, *and those listed above* will not identify the information or contact the individuals. *[45 C.F.R. § 164.514(e)(4)(ii)(c)(5)]*
- I, *and those listed above* agree not to use or further disclose the information in a manner that would violate any requirement of the HIPAA Privacy Rule, 45 C.F.R. Parts 160 and 164. *[45 C.F.R. § 164.514(e)(4)(ii)(A)]*
- I *and those listed above* agree to return all data covered by this agreement to DBH at the conclusion of the project, or to fully document that it was destroyed and the means of its destruction. *[45 C.F.R. § 164.512(i)(2)(ii)(G)]*

Requestor Signature:	**Date:**
DocuSigned by: Christopher Schreus 750BFCCE4C354EE...	12/2/2021

RRC Chair Signature:	**Date**
DocuSigned by: Anthoula Poulakos 8840B829DBE941F...	12/2/2021

Title of Project **mConnect – A Proof of Concept Study for an MDD Dig**

Researcher **Holmusk/Scott Kollins**

Application Submission Checklist

Because DBH receives many requests for data, access to clients, and research support, a structured approach to handling these requests has been developed. To ensure your application receives prompt, careful attention, please use and submit this checklist with your application packet.

	Yes	N/A
1. If you are a student, your application packet includes a letter from your advisor or instructor clearly indicating that your proposed research (A) has been reviewed and (B) meets the research standards of your university.	☐	☒
2. Your proposal specifies your research design and shows why it is the appropriate design for this kind of research.	☒	☐
3. Your literature review is no longer than necessary to show that the research you propose is (A) important (B) derives from previous research activities, and (C) will likely contribute new knowledge to the field.	☐	☒
4. If your design requires statistical procedures, you have consulted with people knowledgeable in this area to ensure that you have chosen the right statistic.	☒	☐
5. If you are using a research hypothesis, it is clearly stated.	☐	☒
6. You have already consulted with DBH staff at the sites you are interested in using in your research.	☒	☐
7. You have built enough time into your research design that you will not likely run into serious time pressures due to the lengthy review and authorization processes at DBH.	☒	☐
8. If your research will involve direct contact with clients, you have prepared and attached a comprehensive *Consent to Participate* form that satisfies legal and ethical requirements.	☒	☐
9. You have carefully considered potential risk factors and included in your application packet detailed information about how these will be managed.	☒	☐
10.		
11.		
12.		
13.		
14.		
15.		