IAP | Medicaid Innovation Accelerator Program

Appendix 2: State Data Use Agreement Example (Georgia)

Introduction

Data sharing is a critical component of many payment and delivery system reform efforts, particularly for those targeting Medicaid Beneficiaries with Complex Care Needs and High Costs (BCNs). To help states pursuing inter-agency data use, the Centers for Medicare & Medicaid Services (CMS) Medicaid Innovation Accelerator Program (IAP) created a resource brief (housed on the IAP Improving Care for Medicaid Beneficiaries with Complex Care Needs and High Costs webpage) on Data Privacy, Data Use and Data Use Agreements. The brief highlights some of the challenges faced by states as well as several resources that states participating in the IAP BCN program area found useful in developing DUAs. These resources include state DUA examples, such as the one featured here from Georgia. States embarking on inter-agency data use can leverage these tools as they pursue data sharing as part of their Medicaid delivery system reform efforts.

EXCERPTS FROM

STATE OF GEORGIA INTERAGENCY MASTER AGREEMENT

BETWEEN

THE GEORGIA DEPARTMENT OF COMMUNITY HEALTH

AND

THE GEORGIA DEPARTMENT OF PUBLIC HEALTH

FOR

DATA SHARING AND DUAL USE

THIS INTERAGENCY MASTER AGREEMENT (hereinafter referred to as "Agreement"), is made and entered into by and between the Georgia Department of Community Health (hereinafter referred to as "DCH") and the Georgia Department of Public Health (hereinafter referred to as "DPH"), each individually a "Party" and collectively referred to as the "Parties", and shall be effective upon the date of last signature by the authorized representatives of the Parties (hereinafter referred to as the "Effective Date").

WHEREAS, DCH is responsible for health care policy, purchasing, planning and regulation pursuant to the Official Code of Georgia Annotated (O.C.G.A.) § 31-2-1 et seq.;

WHEREAS, DCH is the single state agency designated to administer Medical Assistance in Georgia under Title XIX of the Federal Social Security Act, as amended, and O.C.G.A. § 49-4-140 et seq. (the "Medicaid Program"), and is charged with ensuring the appropriate delivery of health care services to Medicaid and PeachCare for Kids® Members;

WHEREAS, DCH is responsible for the administration of the State Health Benefit Plan (the "SHBP") pursuant to the authority granted in O.C.G.A. §§ 45-18-1 et seq., §§ 20-2-880 et seq. and §§ 20-2-910 et seq.;

WHEREAS, DCH provides health benefits under the SHBP for certain current and former State employees, public school teachers and employees, and certain other employees pursuant to State law, as well as their dependents;

WHEREAS, DPH, established July 1, 2011, is empowered to safeguard and promote the health of the people of this State and employ all legal means appropriate to that end pursuant to O.C.G.A. § 31-2A-1 et seq.;

WHEREAS, to carry out the common mission of improving health throughout the State of Georgia, DCH and DPH desire to share certain data, including patient health information;

WHEREAS, pursuant to O.C.G.A. § 31-2A-4, DPH is authorized to exchange data with DCH for purposes of health improvement and fraud prevention for programs operated by DCH pursuant to mutually agreed upon data sharing agreements and in accordance with federal confidentiality laws relating to health care;

WHEREAS, in order to secure the data; in order to ensure the integrity, security, and confidentiality of information maintained by the Parties; and to permit appropriate disclosure and use of such data as permitted by law, DCH and DPH enter in this Agreement; and

WHEREAS, the Parties, as State Entities, are exempt from State Purchasing Requirements and may contract directly between and among each other as set forth in the Georgia Constitution, Article IX, Section ill, Paragraph I.

NOW THEREFORE, for and in consideration of the mutual promises of the Parties, and the terms provisions and conditions of this Agreement, and other good and valuable

consideration, the sufficiency of which is hereby acknowledged, the Parties hereby agree as follows:

I. DEFINITIONS

Data - electronic set of combined elements representing Medical Eligibility and Claims File(s) and Vital Birth and Death Records File(s), gathered from the data defined in the Supplements specified in ***Section III, Data Description***.

Data Owner - the Party (DCH or DPH) that furnishes the Data provided pursuant to the Supplements specified in ***Section III, Data Description,*** is the owner of that Data and retains all ownership rights to their own Data referred to in this Agreement.

II. SCOPE AND PURPOSE

This Agreement addresses the conditions under which the Parties will obtain, use, reuse, and disclose the Data specified in ***Section III, Data Description***, or any derivative file(s) that contain direct individual identifiers or elements that can be used in concert with other information to identify individuals. This Agreement supersedes any and all agreements between the Parties with respect to the use of Data specified in Section Ill and preempts and overrides any instructions, directions, agreements, or other understanding in or pertaining to any prior communication between the Parties with respect to the Data specified herein. The Parties agree further that instructions or interpretations issued concerning this Agreement or the Data specified herein, shall not be valid unless issued in writing by the Parties' contact person specified in ***Section XIII, Notice.***

III. DATA DESCRIPTION

A. The Data covered by this Agreement is defined in Supplements (each Supplement, as it may be amended, modified, extended, or restated from time to time, the "Supplement" and collectively the "Supplements") attached to this Agreement which are hereby incorporated by reference into this Agreement as if fully written herein. In the event the Parties desire to establish additional Data sharing arrangements, the Parties will enter into a Supplement or Supplements to this Agreement. Each existing and newly created Data sharing arrangement shall be governed by the terms and conditions contained in this Agreement.

B. In the event either Party determines that a Data sharing arrangement or activity provided for in the Supplements or in this Agreement cannot be performed, a formal written notice will be provided to the contact person specified in Section XIII, Notice no less than thirty (30) calendar days prior to the deletion of the arrangement or suspension or termination of the activity. The Parties agree to provide a reasonable time period to review any new proposed Data sharing arrangements and to make a decision about whether to add a new Supplement.

IV. PERMITTED PURPOSES

Each Party represents and warrants that it shall, in compliance with applicable law, request, receive, disclose, transmit, and use the Data specified in ***Section III, Data***

Description only for the purpose of performing its obligations under the Supplements and this Agreement, as expressly provided herein.

V. OWNERSHIP OF DATA

The Parties mutually agree that the Party that furnishes the Data provided pursuant to the Supplements specified in Section III, Data Description is the owner of that Data and such Party retains all ownership rights to their own Data referred to in this Agreement, and that no Party obtains any right, title, or interest in any of the Data furnished by the other Party. The Parties further acknowledge and agree that during the term of this Agreement each Party shall have complete editorial freedom with respect to the form and content of their own Data and that each Party may alter their own Data from time to time in its sole discretion.

VI. DCH RESPONSIBILITIES

A. Share securely with DPH the Data (i.e., Medicaid Eligibility and Claims File(s) and supporting enrollment and reference files) described in Section III as defined in the Supplements.

B. Provide a single point of contact for each Data sharing arrangement, as defined in the Supplements to provide on-going guidance and project coordination within DCH.

C. Permit only authorized DCH personnel or vendor, access to the Data of DPH. For purposes of this Agreement, authorized personnel shall mean any person(s) (including but not limited to any employee or support staff member of DCH) identified in Attachments A-l/A-2, as defined in the Supplements. DCH agrees to limit access to the Data to the minimum amount of individuals necessary to achieve the purposes stated in the Supplements (i.e. individuals access to the data will be on a need to know basis).

D. Comply with the provisions of the following attachment, which is hereby incorporated by reference. This Attachment applies to this Agreement, Supplement(s) and any amendments thereto unless otherwise specified therein:

Attachment A: DPH Form GC-00901A, Business Associate Agreement.

VII. DPH RESPONSIBILITIES

A. Share securely with DCH the Data (i.e., Vital Birth and Death Records File(s)) in Section III as defined in the Supplements.

B. Provide a single point of contact for each Data sharing arrangement, as defined in the Supplements to provide ongoing guidance and project coordination within DPH.

C. Permit only authorized DPH personnel or vendor, access to the Data of DCH. For purposes of this Agreement, authorized personnel shall mean any person(s) (including but not limited to any employee or support staff member of DPH) identified in **Attachments B - 1/B-2,** as defined in the Supplements. DPH agrees to limit access to the Data to the

minimum amount of individuals necessary to achieve the purposes stated in the Supplements (i.e. individuals access to the data will be on a need to know basis).

D. Comply with the provisions of the following attachments, which are hereby incorporated by reference. These Attachments apply to this Agreement, Supplement(s), and any amendments thereto unless otherwise specified therein:

Attachment B: DCH Business Associate Agreement

Attachment C: DCH Policy and Procedure 419 Appropriate Use of Information Technology Resources

Attachment D: DCH Procedure 435 Managing Authorization, Access and Control of Information Systems

VIII. DCH/DPH RESPONSIBILITIES

A. Instruct and train each Party' s personnel (including agent(s)[1]) granted access privileges to the Data regarding the confidential nature of the information, the safeguard requirements of this Agreement and other similar State and federal obligations. This includes providing copies of written procedures, standards, policy memorandum, guidelines, and other material which are necessary and pertinent to maintain the confidentiality and restrict the disclosure or re -disclosure of the Data.

B. Enforce the provisions of this Agreement, including, but not limited to any provisions regarding limitations on the Permitted Purposes for access to the Data and any confidentiality provisions of this Agreement by taking any and all disciplinary, remedial, or legal action against any individual who violates such provisions in accordance with this Agreement.

C. Abide by any requirements mandated by the Privacy Rule and the Health Insurance and Portability Act of 1996, Pub. L. No. 104- 191 (hereinafter referred to as HIPAA") or any other applicable laws in the course of this Agreement, including but not limited to:

(1) cooperating with the other Party' s Privacy officials and other compliance officers as required by HIPAA and its regulations; and

(2) signing any other documents that may be required for HIPAA compliance and abiding by their terms and conditions, including but not limited to ***Attachments A*** and ***B.***

D. Establish appropriate administrative, technical, and physical safeguards to protect the confidentiality of the Data and to prevent unauthorized use or access to it. The safeguards shall provide a level and scope of security that is compliant with HIPAA privacy and security standards, as amended, and Title XIII of the American Recovery and Reinvestment

[1] For purposes of this Agreement, the term " agent" shall mean an employee, individual, or entity that is working for and on behalf of a Party in the performance of this Agreement, including but not limited to, temporary staff, consultants, contractors, interns, and/ or third -party intermediaries.

Act of 2009 (the Health Information Technology for Economic and Clinical Health Act, or "HITECH"), and the implementing regulations of HIPAA and HITECH. Implementing regulations are published as the Standards for Privacy and Security of Individually Identifiable Health Information in 45 C.F.R. Parts 160 and 164.

(1) The Parties acknowledge that the use of unsecured communications, including the Internet, to transmit individually identifiable or deducible information derived from the Data specified in Section III is prohibited. Further, the Parties agree that the Data shall not be physically moved, transmitted or disclosed in any way from the authorized project site(s) without written approval from the Data Owner unless such movement, transmission or disclosure is required by law or by a court of competent jurisdiction. Information in electronic format such as magnetic tapes or disks shall be stored in a physically secure environment and processed in such a way that unauthorized persons cannot retrieve the information by means of computer or remote terminal, nor able to view, print, or copy the information.

(2) In the event the Parties will ·utilize a third-party intermediary(ies) (e.g., application service provider, Internet service provider or other network provider) for the purpose of transmitting requests for, receiving, archiving, storing, hosting, or otherwise performing processing of any kind related to the Data, the Parties shall ensure they have first entered into an agreement with such third-party intermediary(ies) prohibiting their use of, and access to the Data for any purpose other than to the extent necessary to carry on the purpose(s) specified in the Supplements. If applicable, the Parties shall also be responsible for requiring their third-party intermediary(ies) to implement safeguards to protect the privacy and security of personal information and protected health information obtained from or given access to by the Data Owner, including ensuring that their third-party intermediary(ies) employ security mechanisms that are consistent with the applicable Security Standards of the HIPAA Regulations. Further, the Parties shall not permit any third-party intermediary(ies) to store, transmit, or access any Data outside of the United States of America.

E. Encrypt the Data during transmission using an encryption methodology that complies with National Institute of Standards and Technology (NIST), AES Encryption Standard, FIPS 197.

F. Grant access to the Data or access to enter the project site(s) where the Data are accessed, stored or processed to the authorized representatives of the other Party for the purpose of inspecting to confirm compliance with the terms of the Agreement; for instance, to verify that necessary and appropriate safeguards are maintained for the protection of the confidentiality and security of the Data[2]. Additionally, during the term of this Agreement, each Party may review the other Party's policies, procedures, practices, and records which pertain to this Agreement if it has good faith reason to believe that such Party is not in compliance with its obligations under this Agreement and that such non-compliance has or

[2] DPH shall not be granted access to enter, for any purpose(s), the project sites) where the State Health Benefit Plan. Data are accessed, stored or processed.

is likely to result in the misuse/wrongful disclosure of or security risk to the Data. Site visits will be coordinated between the Parties and a mutually convenient arrangement will be made, as applicable. Refusal to allow the requesting Party or Party's audit or access for site visits or refusal to schedule a convenient site visit after three (3) attempts may result in termination of this Agreement. The fact that a Party inspects, or fails to inspect, or has the right to inspect the other Party's project site(s), systems, and procedures does not relieve the latter of its responsibility to comply with this Agreement. Nor does a Party's (1) failure to detect or (2) detection of, but failure to notify the other Party or require the other Party's remediation of, any satisfactory practices constitute acceptance of such practice or a waiver of former's enforcement or termination rights under this Agreement. Failure to immediately respond to, comply with, and implement all audit recommendations shall result in immediate termination of this Agreement.

G. Not disclose direct findings, listings, or information derived from the Data specified in Section III, with or without direct identifiers, if such findings, listings or information can, by themselves or in combination with other Data, be used to deduce an individual's identity. (Examples of such data elements include, but are not limited to names, geographic location, age if over 89, sex, diagnosis and procedure, admission/discharge date(s), or date of death.) Moreover, the findings, listings or information shall not be sold, distributed or otherwise made available to any entity or individual (not a party to this Agreement), specifically including but not limited to any posting on the internet, the World Wide Web, social media feeds, or on a third- party website without written approval from the other Party. The Parties agree. further that the Data Owner shall be the sole judge as to whether any finding, listing, information, or any combination of data extracted or derived from their own Data identifies or could, with reasonable effort, be used to identify an individual.

H. Except as specifically authorized in each Supplement, not attempt to match or link records included in the Data specified in Section III to any other individually identifiable source of information. This includes attempts to link the Data to other Party Data. A written protocol that includes the linkage of specific files that has been approved in accordance with the Supplements constitutes express authorization from the Parties to link files as described in the protocol.

I. Submit to the other Party a copy of all findings with respect to the Data, including but not limited to its utilization and disclosure, within thirty (30) calendar days of making such findings. The Parties mutually agree that a Party has made findings with respect to the Data covered by this Agreement when such Party prepares any report or other writing for submission (including, but not limited to, any manuscript to be submitted for publication) concerning any purpose specified in the Supplements (regardless of whether the report or other writing expressly refers to such purpose, to the Data specified in Section III, or any data derived therefrom). The Parties shall not submit such findings to any entity or individual (not a party to this Agreement) until the release of such findings has been approved for each submission, report, publication, or presentation in writing by the Parties' contact specified in **Section XIII, Notice** of this Agreement.

(1) In the event a Party receives a public records request pursuant to any independent Freedom of Information legislation (including but not limited to the Freedom of

Information Act ("FOIA"), 5 U.S.C. § 552 and/or the Georgia Open Records Act, O.C.G.A. § 50-18-71, et. seq.) while this Agreement is in effect or after the termination of this Agreement for any information relating to this Agreement, the Data, or any findings or reports, the Party shall, on the same business day, provide a copy of the Open Records Act request to the other Party's Open Records Officer and Privacy and Security contact specified in ***Attachments A and B***, as well as the other Party's contact person listed in ***Section XIII, Notice***. The Party which receives the Open Records Act request further agrees to comply with the response requirements, restrictions, and exceptions in the applicable statute(s) under which the request is made. Tue Parties will cooperate with each other to ensure that both Parties' interests are represented and that the confidentiality of the Data is not compromised by any actions or omissions by one Party in relation to the public records request or responses thereto. If one Party objects and the other Party is still required by law to disclose the information, the latter shall do so only to the minimum extent necessary to comply with the operation of the law, and shall provide the objecting Party a copy of the information disclosed.

J. Not reuse original or derivative Data. Tue Data Owner shall make such determination regarding approval and notify the other Party within ten (10) business days after receipt of a written request for reuse of original or derivative Data.

K. Comply and abide by all federal and state laws, rules, regulations, statutes, case law, precedent, policies, or procedures that may govern the Agreement, or either Party's responsibilities. To the extent that applicable federal and state laws, rules, regulations, statutes, case law, precedent, policies, or procedures - either those in effect at the time of the execution of this Agreement, or those which become effective or are amended during the life of the Agreement - require a Party to take action or inaction, any costs, expenses, or fees associated with that action or inaction shall be borne and paid by such Party solely.

L. In the event the Data Owner determines or has a reasonable belief that the other Party or its agent(s) has made or may have made a use, reuse or disclosure of the aforesaid file(s) that is not authorized by this Agreement, the Data Owner, at its sole discretion, may require the other Party to: (a) promptly investigate and report to the Data Owner their determinations regarding any alleged or actual unauthorized use, reuse or disclosure, (b) promptly resolve any problems identified by the investigation; (c) submit a formal, written response to an allegation of unauthorized use, reuse or disclosure; (d) submit a corrective action plan with steps designed to prevent any future unauthorized uses, reuses or disclosures; and/or (e) return or destroy the Data it received under this Agreement. The Data Owner reserves the right to require immediate cessation of such use, reuse, or disclosure until the matter is fully investigated and corrective action, if required, has been taken by the other Party.

M. Promptly notify the other Party of any breach of security concerning confidential information and cooperate fully in the federal security incident process.

N. Share information regarding outcomes and results with the other Party, in addition to any report(s) reasonably requested for purposes of monitoring Data use. The content and format of the reports shall be established by mutual agreement of the Parties.

O. Facilitate discussions between the Parties to further the purposes of this Agreement, including but not limited to:

(1) cooperating fully with the other Party with respect to activities as they relate to this Agreement;

(2) devoting such time as may be reasonably requested by the other Party to review information, meet with, respond to, and advise the other Party with respect to activities as they relate to this Agreement;

(3) providing such reasonable assistance as may be requested by the other Party when performing activities as they relate to this Agreement; and

(4) subject to the other Party's right to restrict or condition its cooperation or disclosure of information in the interest of preserving privileges in any foreseeable dispute or litigation or protecting such Party's proprietary information, provide information and assistance to the other Party in the investigation of breaches and disputes.

P. Take such action as is necessary to amend this Agreement from time to time as is necessary for either Party or both Parties to comply with changes to HIPAA, federal or State statute, or regulation.

IX. TERM

This Agreement shall begin on the Effective Date and shall continue until June 30, 2015, and shall automatically renew annually for additional one-year terms, not to exceed fifty (50) years, unless terminated earlier pursuant to Section X, Termination. Notwithstanding the above, the term specified in the Supplement shall control the termination of the exchange of the Data therein.

X. TERMINATION

A. This Agreement may be terminated by either Party at any time, in its sole discretion, for any reason upon thirty (30) calendar days' written notice, pursuant to ***Section XHI, Notice***. Either Party may immediately terminate this Agreement if it in good faith, determines that (1) the other Party, either directly or indirectly, has materially breached any of its obligations under this Agreement; (2) there is a substantial likelihood that the other Party's acts or omissions create an immediate threat or will cause irreparable harm to an individual whose personal health information is disclosed; (3) the requirements of any law, regulations and/or judicial action have not been met; and/or (4) as a result of changes in laws, regulations or regulatory or judicial action, that the requirements of any law, regulation or judicial action will not be met. Upon notice of termination, both Parties shall be released of any and all obligations under this Agreement. Failure to immediately respond to, comply with, and implement all audit recommendations shall result in

immediate termination of this Agreement. In the event of termination of this Agreement, all Supplements will also terminate. However, any Supplement may be terminated by the Parties or expire pursuant to its own terms without requiring or causing the termination of this Agreement unless specifically set forth by one or both Parties in accordance with this Section.

B. Upon termination or expiration of this Agreement, whichever occurs sooner, or the termination or expiration of any Supplement, the Data Owner will notify the other Party to either return all Data or to destroy such Data via a method to be specified by the Data Owner, including but not limited to (a) destroying links in its possession, custody or control, (b) removing Data (including derived datasets) from all systems, sites and/or software, (c) pulping or cross-shredding printed information, and (d) pulverizing or incinerating CDs, tapes, disks, and other such non-paper media. If the Data Owner elects to have the other Party destroy the Data, the latter shall destroy and send written certification of the destruction to the Data Owner within thirty (30) calendar days of receiving instruction. Notwithstanding the foregoing, the Data Owner reserves the right to attend or audit the destruction of the Data. If the Data Owner elects to have the Data returned, the other Party shall return all Data and any derivative Data within thirty (30) calendar days of receiving notice to that effect. Said Party shall not retain the Data or any parts thereof (whether in paper, electronic, or any form, and regardless of medium on which such Data· is stored), after the aforementioned Data is returned or destroyed.

   (1) If, however, it is determined that returning or destroying the Data is not feasible or if the Data Owner has not notified the other Party to return or destroy the Data, then the retaining Party must maintain the privacy protections under the Data Owner's Business Associate Agreement and other provisions of this Agreement relating to protection of Data and according to applicable law as long as said Party retains the Data. Similarly, if a Party determines that it is infeasible to obtain the Data in its third-party intermediary(ies) possession, it must provide a written explanation to the Data Owner of such reasons and require its third -party intermediary(ies) to agree to extend any and all protections, limitations and restrictions contained in this Agreement and in the Data Owner’s Business Associate Agreement to such third -party intermediary(ies)' use or disclosure of any Data retained after the termination of this Agreement, and to limit any further uses or disclosures for the purposes that make the return or destruction of the Data infeasible.

XI. LIABILITY

A. The Parties hereby acknowledge that civil and/ or criminal penalties under State and federal law, including fines, imprisonment or both, may apply to unauthorized disclosures of individually identifiable information.

B. Each Party assumes responsibility for the confidentiality and security of the information or Data, and shall be liable for its own acts and omissions (and those of its agent(s)) and any penalties and/ or fines incurred by the other Party arising there from due to non-compliance with any state and federal laws, rules, procedures and regulations (including any amendments). No Party will be liable for the acts or omissions of the other Party.

XII. PERIODIC REVIEW

C. The Parties will jointly evaluate progress in the implementation and maintenance of the Agreement (including reviewing and evaluating the Data sharing arrangements, as defined by the Supplements) and revise and develop objectives, decisions and processes as appropriate to explore other avenues of interaction between the Parties.

D. The Parties may establish a coordinating committee consisting of the Commissioner or his or her designee from DCH, the Commissioner or his or her designee from DPH, and a representative of each appropriate program division of DCH and DPH. The Committee, at its discretion, may set up subcommittees to research and develop recommendations for solutions to pertinent issues.

XIII. NOTICE

A. The following named individuals will be designated as point -of - contact for his or her respective entities:

For DCH:

Division of Medical Assistance Plans
Medicaid Deputy Chief, Policy and Provider Services
Georgia Department of Community Health, Division of Medicaid

State Health Benefit Plan Division
Deputy Chief, State Health Benefit Plan Division
Georgia Department of Community Health

For DPH:
Chief of Staff
Georgia Department of Public Health

B. All notices given hereunder shall be in writing, and shall be deemed to be duly given if delivered by any of the following methods:

(1) by personal delivery;
(2) by electronic mail or facsimile, with a confirmation copy sent by first class mail;
(3) registered or certified mail, postage prepaid, return receipt requested; or
(4) by a nationally recognized overnight courier.

C. A notice sent by certified mail or express courier shall be deemed given on the date of receipt or refusal of receipt. A notice sent by electronic mail or facsimile shall be deemed given on the date of electronic confirmation of receipt, or deemed delivered in the absence of confirmation that delivery did not occur.

D. In the event that a Party decides to identify a new or additional point -of -contact, the respective Commissioner or his or her designee will send written notification to the other

Party identifying, the name, title, and address of the new point -of -contact. Identification of a new point -of -contact is not considered an amendment to this Agreement.

XIV. INTERPRETATION

This Agreement shall be governed by, construed, and applied in accordance with the laws of the State of Georgia. Any ambiguity in this Agreement shall be resolved in favor of a meaning that complies and is consistent with applicable law protecting the privacy, security and confidentiality of the Data, including but not limited to HIPAA and the HIPAA regulations. Moreover, the terms of this Agreement shall be construed in light of any applicable interpretation or guidance on HIPAA or the Privacy Rule issued by the Department of Health and Human Services or its Office of Civil Rights from time to time.

XV. DISPUTE RESOLUTION

The Parties agree to attempt in good faith to promptly resolve any dispute, controversy or claim arising out of or relating to this Agreement and to amicably settle any differences expediently without any disruption in service through negotiations between the Parties. Outstanding issues shall be resolved between the departmental unit management as appropriate. If no resolution can be reached at the appropriate unit level, the issue will be escalated to upper/senior management for resolution. If no resolution can be reached at the upper/senior management level, the issue will be escalated to the commissioner level for resolution.

XVI. FUNDING

It is expressly understood that neither Party shall have any financial obligation arising from this Agreement, except to the extent it incurs its own charges related to protection of the Data or as a result of non-compliance with the terms of the Agreement as specified herein. Any proposed or amended Supplement which requires a financial obligation in addition to the aforementioned will need to be strictly and solely approved by each Party's Commissioner or his or her designee.

XVII. COUNTERPARTS

This Agreement may be executed in two original counterparts, which shall constitute one and the same instrument. Any signature below that is transmitted by facsimile or other electronic means shall be binding and effective as the original.

XVIII. AMENDMENT

No amendment of this Agreement, or any of its Supplements, or any of the terms or provisions hereof, shall be binding upon either Party except by a writing executed by both Parties. Any Supplement to this Agreement may be amended separately, in writing, by referencing this provision, provided that both Parties sign or initial, as applicable, the Supplement as amended.

XIX. ORDER OF PRECEDENCE

In the event of any conflict between this. Agreement and any Supplement, exhibit or attachment incorporated into this Agreement, the provisions of this Agreement shall control and govern, except that the terms of the Data Owner' s Business Associate Agreement shall govern, for the express and agreed upon purpose of compliance with the more stringent protections of confidentiality, privacy, and security of the Data defined in the Supplements.

XX. SURVIVABILITY

The terms, provisions, representations and warranties contained in this Agreement shall survive any expiration or termination of this Agreement and/ or its Supplements. Expressly, the obligations set forth in ***Attachments A and B (Business Associate Agreements) and Sections IV (Permitted Purposes), V (Ownership and Control of Data), VI (DCH Responsibilities), VII (DPH Responsibilities), VIII (DCHIDPH Responsibilities), and XI (Liability)*** herein shall survive termination of, or expiration of, this Agreement or the Supplements.

XXI. SEVERABILITY

Any section, subsection, paragraph, term, condition, provision or other part (hereinafter collectively referred to as " part") of this Agreement that is judged, held, found, or declared to be voidable, void, invalid, illegal or otherwise not fully enforceable shall not affect any other part of this Agreement, and the remainder of this Agreement shall continue to be of full force and effect.

XXII. ASSIGNMENT

No Party may assign this Agreement, in whole or in part, without the prior written consent of the other Parties, and any attempted assignment not in accordance herewith shall be null and void and of no force or effect.

XXIII. ENTIRE AGREEMENT

This Agreement, together with any documents incorporated herein, constitutes the entire agreement between the Parties with respect to its subject matter hereof and supersede all other prior and contemporaneous statements, instructions, directions, agreements, and understandings between the Parties regarding its subject matter. No written or oral statements, agreements, or understandings that are not set out, referenced, or specifically incorporated in this Agreement shall in any way be binding or of effect between the Parties.

XXIV. PARTIES BOUND

This Agreement is binding upon all employees, agents and third -party vendors of DCH and DPH and will bind the respective heirs, executors, administrators, legal representatives, successors and assigns of each Party.

(Signatures on following page)

SIGNATURE PAGE

IN WITNESS WHEREOF, DCH and DPH, through their authorized officers and agents, have caused this Agreement to be executed on their behalf as of the date indicated.

GEORGIA DEPARTMENT OF COMMUNITY HEALTH

GEORGIA DEPARTMENT OF PUBLIC HEALTH

ATTACHMENT A - DPH FORM GC -00901A: BUSINESS ASSOCIATE AGREEMENT

WHEREAS, the Georgia Department of Public Health (" DPH") and the Georgia Department of Community Health (" Contractor") have entered into the attached Contract, whereby Contractor will provide functions, activities, or services to DPH involving the use of Protected Health Information (' PHP') as defined by Health Insurance Portability and Accountability Act of 1996 HIPAA");

WHEREAS, DPH is required by HIPAA to enter into a Business Associate Agreement with entities which provide functions, activities, or services on behalf of DPH involving the use of PHI;

NOW, THEREFORE, in consideration of the mutual promises contained herein, DPH and Contractor agree as follows:

1. Terms used but not otherwise defined in this Agreement shall have the same meaning as those terms in HIPAA and Title XIII of the American Recovery and Reinvestment Act of 2009 (the Health Information Technology for Economic and Clinical Health Act, or HITECH"), and in the implementing regulations of HIPAA and HITECH, now and as they may be amended in the future. Together HIPAA, HITECH, and their implementing regulations are referred to in this Agreement as the “Privacy Rule and the Security Rule."

2. Subject to the limitations of this Agreement, Contractor may use or disclose PHI only to the extent necessary to meet its responsibilities as set forth in the Contract, provided that such use or disclosure would not violate the Privacy Rule or the Security Rule if done by DPH.

3. Contractor warrants that the individuals described on Attachment A-1 require access to PHI in order to perform services under the Contract. Contractor shall update Attachment A-1 as necessary.

4. Contractor warrants that the individuals described on Attachment A-2 require access to a DPH information system in order to perform services under the Contract. Contractor shall notify the DPH Project Leader no less than 24 hours in advance if any other individuals will need access to the DPH information system.

5. Contractor warrants that only individuals designated by title or name on Attachments A-1 and A-2 will request or access PHI from DPH, that they will only do so in the performance of services under the Contract, and that these individuals will only request the minimum necessary amount of information in order to perform those services.

6. The parties agree that Contractor is a "Business Associate" to DPH within the meaning of the Privacy and Security Rule. Contractor shall comply with all obligations of the Privacy Rule and Security Rule that apply to DPH, and shall comply with all Privacy Rule and Security Rule requirements that apply to Business Associates. Contractor further warrants that it maintains and follows written policies and procedures to achieve and maintain compliance with the Privacy and Security Rules that apply to Business Associates, and that it will update such policies and procedures as necessary in order to comply -with the and changes to the Privacy and Security Rules. These policies and procedures, and evidence of their implementation, shall be provided to DPH upon request.

7. All communications related to compliance with this Agreement will be forwarded to the following Privacy and Security Contacts:

   A. At DPH: HIPAA Privacy Officer, Office of General Counsel

      Deputy Chief Information Officer, Office of Information Technology

   B. At Contractor: HIPAA Privacy and Security Specialist, Office of General Counsel

      Agency Information Security Officer

8. Contractor further agrees:

   A. Contractor will not request, create, receive, use or disclose PHI other than as permitted or required by this Agreement, the Contract, or law.

   B. Contractor will establish, maintain and use appropriate administrative, physical, and technical safeguards to prevent loss, use, or disclosure of the PHI other than as provided for by this Agreement, the Contract, or law.

   C. Contractor will implement and use administrative, physical, and technical safeguards that protect the confidentiality, integrity and availability of the electronic PHI that it creates, receives, maintains, or transmits on behalf of DPH.

   D. In addition to the safeguards described above, Contractor shall impose access controls that restrict access to PHI to the individuals listed on A- 1 and A-2, as amended from time to time.

   E. Contractor will password -protect and encrypt all electronic PHI for transmission and for storage on portable computers and media devices.

   F. Contractor will mitigate, to the extent practicable, any harmful effect that result from a loss use, or disclosure of PHI by Contractor in violation of the requirements of this Agreement, the Contract, or law. Contractor shall bear the costs of mitigation, which shall include the reasonable costs of credit monitoring or credit restoration when the use or disclosure results in exposure of information commonly used in identity theft including name, date of birth, and Social Security Number.)

G. Contractor will maintain a written Business Associate Agreement with any agent or subcontractor that will create, receive, maintain, or transmit on Contractor's behalf any PHI pertaining to DPH. Such Agreement shall provide that Contractor's agent or subcontractor agrees to the same restrictions and conditions of this Agreement with respect to PHI that Contractor receives from DPH, and that Contractor's agent or subcontractor assumes the same duties with regard to the PHI that Contractor has assumed under this Agreement. Contractor further agrees that if it becomes aware of a pattern of activity or practice of its agent or subcontractor that constitutes a material breach or violation of its agreement with Contractor, then Contractor shall take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, terminate the agreement.

H. Contractor will immediately report to DPH any "Breach" as defined by 45 CFR 164.402, and any known or suspected loss, use, or disclosure of PHI that is not authorized by this Agreement, the Contract, or law.

I. Make an initial report to DPH in writing in such form as DPH may require within three business days after Contractor learns of a suspected unauthorized loss, use, or disclosure of PHI. This report will include the following:

   i. The nature of the loss, use, or disclosure, a brief description of what happened, the date it occurred, and the date Contractor discovered the incident;

   ii. The specific data points of PHI involved in the loss, use, or disclosure;

   iii. The names of all persons with knowledge of the loss, use, or disclosure, and the names or categories of persons who may have obtained access to the PHI as a result;

   iv. The corrective or investigative actions taken or to be taken in order to mitigate harmful effects, and to prevent further losses, uses, or disclosures;

   v. Recommended protective actions to be taken by individuals whose PHI may have been lost, used, or disclosed; and

   vi. Whether Contractor believes that the loss, use, or disclosure constitutes a Breach.

J. Contractor will, upon request by the DPH Privacy Officer or the DPH Information Security Officer, provide a complete report of the Breach to DPH including a root cause analysis and a proposed corrective action plan. Upon request by DPH, Contractor shall implement the corrective action plan and provide proof of implementation.

K. Contractor will report to the DPH Privacy Officer and the DPH Information Security Officer any successful unauthorized access, modification, or destruction of PHI or interference with system operations in Contractor' s information systems as soon as practicable but in no event later than three business days of discovery.

L. Contractor will cooperate with DPH and provide assistance necessary for DPH to determine whether a Breach has occurred, and whether notification of the Breach is legally required or otherwise appropriate.

M. If DPH determines that a Breach has occurred as a result of Contractor's loss, use, or disclosure of PHI or failure to comply with obligations set forth in this Agreement or in the Privacy or Security Rule, then Contractor will provide all required notices to affected individuals, the Secretary of the U. S. Department of Health and Human Services, and the media, at Contractor's expense and in accordance with 45 C.F.R. Part 164 subpart D. Such notices shall be submitted in advance to the DPH Privacy Officer for approval.

N. Contractor will honor requests by DPH or by an individual for access to the individual' s own PHI in accordance with 45 CFR 164.524; to make PHI available for amendment, and to incorporate such amendments into a designated record set in accordance with 45 CFR 164. 526; to provide an accounting of all disclosures of the individual' s PHI in accordance with 45 CFR 164.528; to document any such requests and the Contractor' s response; and to notify DPH as soon as practicable of any such requests.

O. Contractor will provide access to the Secretary of the U.S. Department of Health and Human Services to Contractor's books and records and policies, practices, or procedures relating to the use and disclosure of PHI received from DPH, or created or received by Contractor on behalf of DPH.

P. Contractor will work in good faith with DPH to promptly resolve any dispute, controversy or claim arising out of or relating to a violation of the HIPAA Privacy and Security Rules or Breach that arises from the conduct or omission of Business Associates or its employee(s), agent(s) of subcontractor(s). Business Associate acknowledge that such a violation of the HIPAA Privacy and Security Rules of breach of this Agreement may result in financial harm to DPH, including but not limited to, damages, fines, civil penalties and reasonable attorneys' fees imposed on DPH as a result of such conduct or omission. Business Associate agrees to act in good faith to mitigate such financial harm to DPH, including, but not limited to, pursuing or assisting DPH in its pursuit of any financial recovery available through insurance or other financial coverage maintained by the Department of Administrative Services or any successor entity, pursuing any financial recovery available through Business Associate' s contracts with its agents or subcontractors as applicable, or taking such other action as determined reasonable by DPH and the Business Associate taking into consideration State budgetary requirements and restrictions.

9. Unless otherwise provided by law, DPH agrees that it will:

A. Notify Contractor of any new limitation in DPH’s Notice of Privacy Practices in accordance with the provisions of the Privacy Rule if such limitation will affect Contractor's use or disclosure of PHI.

B. Notify Contractor of any change in, or revocation of, permission by an individual for DPH to use or disclose PHI if such change or revocation will affect Contractor's use or disclosure of PHI.

C. Notify Contractor of any restriction regarding its use or disclosure of PHI that DPH has agreed to in accordance with the Privacy Rule if such restriction will affect Contractor's use or disclosure of PHI.

D. Before agreeing to any changes in or revocation of permission by an individual, or any restriction to use or disclose PHI, DPH will contact Contractor to determine feasibility of compliance. DPH agrees to assume all costs incurred by Contractor in compliance with such special requests.

10. The effective date of this Agreement shall be the same as that of the Contract. Unless otherwise terminated, this Agreement shall continue until all of the PHI provided by DPH to Contractor, or created or received by Contractor on behalf of DPH, is destroyed or returned to DPH.

    A. Termination for Cause. Upon violation of a material term of this Agreement by Contractor, DPH may provide an opportunity for Contractor to cure the breach and, if Contractor fails to cure the breach, terminate the contract upon 30 calendar days' notice.

    B. Termination for Convenience. In the event that the Contract is terminated for any reason, then DPH may terminate this Agreement for convenience.

    C. Effect of Termination.

        i. Upon termination of this Agreement, DPH shall determine whether return or destruction of PHI is feasible. If so, then Contractor shall at the direction of DPH either destroy the PHI or to return it to DPH, keeping no copies. If DPH determines that return or destruction is not feasible, then Contractor shall continue to extend the protections of this Agreement to the PHI for as long as Contractor maintains the PHI, and shall limit the use and disclosure of the PHI to those purposes that make the return or destruction of the PHI infeasible.

        ii. The obligations imposed upon Contractor with respect to its care, use, and disclosure of PHI, and its duty to comply with the Privacy and Security Rule with regard to such PHI, shall survive the termination of this Agreement and the termination or completion of the Contract.

11. Nothing in this Agreement is intended to confer any rights, remedies, obligations, or liabilities upon anyone other than DPH and Contractor.

12. This Agreement is intended to supplement, and not to diminish or alter, the terms and conditions of the Contract.

GEORGIA DEPARTMENT OF COMMUNITY HEALTH

ATTACHMENT A-1 - Individuals Permitted to Receive, Use, and Disclose DPH PHI

The following individuals, as employees or agents of Contractor, need access to DPH Protected Health Information in order for Contractor to perform the services described in the Contract:

[Insert list of individuals with position titles]

Approved methods of secure delivery of PHI between Contractor and DPH:

- Secure FTP file transfer (preferred)
- Encrypted email or email sent through " secure tunnel' approved by DPH Information
- Security Officer
- Email of encrypted document (password must be sent by telephone only)
- Encrypted portable media device and tracked delivery method

Contractor must update this list as needed and provide the updated form to the DPH Project Leader. Use of DPH Protected Health Information by individuals who are not described on this Attachment A- 1, as amended from time to time, is a violation of the Agreement.

DPH Project Leader Contact Information:
Chief of Staff

ATTACHMENT A-2 - List of Individuals Authorized to Access a DPH Information System Containing PHI

The following individuals, as employees or agents of Contractor, need access to DPH Information. Systems containing DPH Protected Health Information in order for Contractor to perform the services described in the Contract:

[Insert list of individuals with name of system and type of access]

The DPH Project Leader must submit a completed DPH Network Access Request Form for each individual listed above, and for anyone who might later be added to this list.

Contractor must notify the Project Leader identified in the Contract immediately, but at least within 24 hours, after any individual on this list no longer needs the level of access described. Failure to provide this notification on time is a violation of the Agreement.

Contractor must update this Attachment A-2 as needed and provide the updated form to the DPH Project Leader.

ATTACHMENT B - DCH BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (hereinafter referred to as " Agreement"), effective on [insert Business Associate Agreement Effective Date], (hereinafter the "Effective Date") is made and entered into by and between the Georgia Department of Community Health (hereinafter referred to as " DCH") and the Georgia Department of Public Health (hereinafter referred to as Contractor") as **Attachment A** to **Contract No. 2015002** between DCH and Contractor dated [insert Contract No. 2015002 Effective Date], (hereinafter referred to as the " Contract").

WHEREAS, DCH is a hybrid entity, as defined in the Health Insurance Portability and Accountability Act of 1996, Public Law 104- 191 (" HIPAA"), and is required, by HIPAA to enter into a Business Associate Agreement with certain entities that provide functions, activities, or services on behalf of or in support of health care components of DCH, which functions, activities or services involve the use of Protected Health Information as defined by HIPAA ("PHI");

WHEREAS, Contractor, under the Contract provides functions, activities, or services involving the use of PHI;

NOW, THEREFORE, for and in consideration of the mutual promises, covenants and agreements contained herein, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, DCH and Contractor (each individually a " Party" and collectively the " Parties") hereby agree as follows:

1. Terms used but not otherwise defined in this Agreement shall have the same meaning as those terms have in HIPAA and in Title XIII of the American Recovery and Reinvestment Act of 2009 (the Health Information Technology for Economic and Clinical Health Act, or HITECH"), and in the implementing regulations of HIPAA and HITECH. Implementing regulations are published as the Standards for Privacy and Security of Individually Identifiable Health Information in 45 C.F.R. Parts 160 and 164. Together, HIPAA, HITECH, and their implementing regulations are referred to in this Agreement as the "Privacy Rule and Security Rule." If the meaning of any defined term is changed by law or regulation, then this Agreement will be automatically modified to conform to such change. The term “NIST Baseline Controls" means the baseline controls set forth in National Institute of Standards and Technology (NIST) SP 800-53 established for " moderate impact" information.

2. Except as limited in this Agreement, Contractor may use or disclose PHI only to the extent necessary to meet its responsibilities, as set forth in the Contract provided that such use or disclosure would not violate the Privacy Rule or the Security Rule, if done by DCH. Furthermore, except as otherwise limited in this Agreement, Contractor may:

   A. Use PHI for internal quality control and auditing purposes.

   B. Use or disclose PHI as Required by Law.

C. After providing written notification to DCH' s Office of Inspector General, use PHI to make a report to a health oversight agency authorized by law to investigate DCH (or otherwise oversee the conduct or conditions of the DCH) about, any DCH conduct that Contractor in good faith believes to be unlawful as permitted by 45 C.F.R. 164.5020)(1). Notwithstanding the foregoing, Contractor shall not be required to provide prior written notice to DCH's Office of Inspector General if Contractor is provided written instruction otherwise by the health oversight agency authorized by law to investigate DCH.

D. Use and disclose PHI to consult with an attorney for purposes of determining Contractor's legal options with regard to reporting conduct by DCH that Contractor in good faith believes to be unlawful, as permitted by 45 C.F.R. 164.5020)(1).

3. Contractor represents and warrants that only individuals designated by title or name on **Attachments B- 1** and **B-2** will request PHI from DCH or access DCH PHI in order to perform the services of the Contract, and these individuals will only request the minimum. Necessary amount of information necessary in order to perform the services.

4. Contractor represents and warrants that the individuals listed by title on **Attachment B- 1** require access to PHI in order to perform services under the Contract. Contractor agrees to send updates to **Attachment B-1** whenever necessary. Uses or disclosures of PHI by individuals not described on **Attachment B-1** are impermissible.

5. Contractor represents and warrants that the individuals listed by name on **Attachment B-2** require access to a DCH information system in order to perform services under the Contract. Contractor agrees to notify the Project Leader and the Access Control Coordinator named on **Attachment B- 2** immediately, but at least within 24 hours, of any change in the need for DCH information system access by any individual listed on **Attachment B- 2**. Any failure to report a change within the 24 hour time period will be considered a security incident and may be reported to Contractor's Privacy and Security Officer, Information Security Officer and the Georgia Technology Authority for proper handling and sanctions.

6. Contractor agrees that it is a Business Associate to DCH as a result of the Contract, and represents and warrants to DCH that it complies with the Privacy Rule and Security Rule requirements that apply to Business Associates and will continue to comply with these requirements. Contractor further represents and warrants to DCH that it maintains and follows written policies and procedures to achieve and maintain compliance with the HIPAA Privacy and Security Rules that apply to Business Associates, including, but not limited to policies and procedures addressing HIPAA' s requirements that Business Associates use, request and disclose only the minimum amount of PHI necessary to perform their services, and updates such policies and procedures as necessary in order to comply with the HIPAA Privacy and Security Rules that apply to Business Associates and will continue to maintain and update such policies and procedures. These policies and procedures, and evidence of their implementation, shall be provided to DCH upon request.

7. The Parties agree that a copy of all communications related to compliance with this Agreement will be forwarded to the following Privacy and Security Contacts:

A. At DCH: HIPAA Privacy and Security Specialist
Office of General Counsel

HIPAA Privacy and Security Specialist
Office of General Counsel

Agency Information Security Officer

B. At Contractor: Associate General Counsel, PH/General Counsel

Deputy Chief Information Officer, Office of Information Technology

8. Contractor further agrees that it will:

A. Not request, create, receive, use or disclose PHI other than as permitted or required by this Agreement, the Contract, or as required by law.

B. Establish, maintain and use appropriate administrative, physical and technical safeguards to prevent use or disclosure of the PHI other than as provided for by this Agreement or the Contract. Such safeguards must include all NIST Baseline Controls, unless DCH has agreed in writing that the control is not appropriate or applicable.

C. Implement and use administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of DCH. Such safeguards must include all NIST Baseline Controls, unless DCH has applicable.

D. In addition to the safeguards described above, Contractor shall include access controls that restrict access to PER to the individuals listed on B-1 and B-2, as amended from time to time, shall implement encryption of all electronic PHI during transmission and at rest.

E. Upon DCH' s reasonable request, but no more frequently than annually, obtain an independent assessment of Contractor' s implementation of the NIST Baseline Controls and the additional safeguards required by this Agreement with respect to DCH PHI, provide the results: of such assessments to DCH, and ensure that corrective actions identified during the independent assessment are implemented.

F. Mitigate, to the extent practicable, any harmful effect that may be known to Contractor from a use or disclosure of PHI by Contractor in violation of the requirements of this Agreement, the Contract or applicable regulations. Contractor shall bear the costs of mitigation.

G. Maintain a business associate agreement with its agents or subcontractors to whom it provides PHI, in accordance with which such agents or subcontractors are contractually obligated to comply with at least the same obligations that apply to Contractor under this Agreement, and ensure that its agents or subcontractors comply with the conditions, restrictions, prohibitions and other limitations regarding the request for, creation, receipt, use or disclosure of PHI, that are applicable to Contractor under this Agreement and the Contract.

H. Report to DCH any use or disclosure of PHI that is not provided for by this Agreement or the Contract of which it becomes aware.

I. Make an initial report to the DCH in writing in such form as DCH may require within three (3) business days after Contractor (or any subcontractor) becomes aware of the unauthorized use or disclosure. This report will require Contractor to identify the following:

i. The nature of the impermissible use or disclosure (the " incident"), which will include a brief description of what happened, including the date it occurred and the date Contractor discovered the incident;

ii. The Protected Health Information involved in the impermissible use or disclosure, such as whether the full name, social security number, date of birth, home address, account number or other information were involved);

iii. Who (by title, access permission level and employer) made the impermissible use or disclosure and who received the Protected Health Information as a result;

iv. What corrective or investigational action Contractor took or will take to prevent further impermissible uses or disclosures, to mitigate harmful effects, and to prevent against any further incidents;

v. What steps individuals who may have been harmed by the incident might take to protect themselves; and

vi. Whether Contractor believes that the impermissible use or disclosure constitutes a Breach of Unsecured Protected Health Information.

Upon request by the DCH HIPAA Privacy and Security Officer or the DCH Information Security Officer, Contractor agrees to make a complete report to the DCH in writing within two weeks of the initial report that includes a root cause analysis and a proposed corrective action plan. Upon approval of a corrective action plan by the DCH, Contractor agrees to implement the corrective action plan and provide proof of implementation to the DCH within five (5) business days of DCH's request for proof of implementation.

J. Report to the DCH HIPAA Privacy and Security Officer and the DCH Agency Information Security Officer any successful unauthorized access, modification, or destruction of PHI or interference with system operations in Contractor' s information

systems as soon as practicable but in no event later than three (3) business days of discovery. If such a security incident resulted in a use or disclosure of PHI not permitted by this Agreement, Contractor shall also make a report of the impermissible use or disclosure as described above. Contractor agrees to make a complete report to the DCH in writing within two weeks of the initial report that includes a root cause analysis and, if appropriate, a proposed corrective action plan designed to protect PHI from similar security incidents in the future. Upon DCH's approval of Contractor's corrective action plan, Contractor agrees to implement the corrective action plan and provide proof of implementation to the DCH.

K. Upon DCH's reasonable request and not more frequently than once per quarter, report to the DCH Agency Information Security Officer any (A) attempted (but unsuccessful) unauthorized access, use, disclosure, modification, or destruction of PHI or (B) attempted (but unsuccessful) interference with system operations in Contractor's information systems. Contractor does not need to report trivial incidents that occur on a daily basis, such as scans, "pings," or other routine attempts that do not penetrate computer networks or servers or result in interference with system operations.

L. Cooperate with DCH and provide assistance necessary for DCH to determine whether a Breach of Unsecured Protected Health Information has occurred, and whether notification of the Breach is legally required or otherwise appropriate. Contractor agrees to assist DCH in its efforts to comply with the HIPAA Privacy and Security Rules, as amended from time to time. To that end, the Contractor will abide by any requirements mandated by the HIPAA Privacy and Security Rules or any other applicable laws in the course of this Contract. Contractor warrants that it will cooperate with DCH, including cooperation with DCH privacy officials and other compliance officers required by the HIPAA Privacy and Security Rules and all implementing regulations, in the course of performance of this Contract so that both parties will be in compliance with HIPAA.

M. If DCH determines that a Breach of Unsecured Protected Health Information has occurred as a result of Contractor's impermissible use or disclosure of PHI or failure to comply with obligations set forth in this Agreement or in the Privacy or Security Rules, provide all notifications to Individuals, HHS and/ or the media, on behalf of DCH, after the notifications are approved by the DCH. Contractor shall provide these notifications in accordance with the security breach notification requirements set forth in 42 U.S. C. § 17932 and 45 C. F.R. Parts 160 & 164 subparts A, D & E as of their respective Compliance Dates, and shall pay for the reasonable and actual costs associated with such notifications.

In the event that DCH determines a Breach has occurred, without unreasonable delay, and in any event no later than thirty (30) calendar days after Discovery, Contractor shall provide the DCH HIPAA Privacy and Security Officer a list of Individuals and a copy of the template notification letter to be sent to Individuals. Contractor shall begin the notification process only after obtaining DCH's approval of the notification letter.

N. Make any amendment(s) to PHI in a Designated Record Set that DCH directs or agrees to pursuant to 45 CFR 164. 526 within five (5) business days after request of DCH. Contractor also agrees to provide DCH with written confirmation of the amendment in such format and within such time as DCH may require.

O. In order to meet the requirements under 45 CFR 164. 524, regarding an individual's right of access, Contractor shall, within five (5) business days following DCH's request, or as otherwise required by state or federal law or regulation, or by another time as may be agreed upon in writing by the DCH, provide DCH access to the PHI in an individual' s Designated Record Set. However, if requested by DCH, Contractor shall provide access to the PHI in a Designated Record Set directly to the individual to whom such information relates.

P. Give the Secretary of the U.S. Department of Health and Human Services (the Secretary") or the Secretary's designees access to Contractor's books and records and policies, practices or procedures relating to the use and disclosure of PHI for or on behalf of DCH within five (5) business days after the Secretary or the Secretary's designees request such access or otherwise as the Secretary or the Secretary's designees may require. Contractor also agrees to make such information available for review, inspection and copying by the Secretary or the Secretary's designees during normal business hours at the location or locations where such information is maintained or to otherwise provide such information to the Secretary or the Secretary's designees in such form, format or manner as the Secretary or the Secretary's designees may require.

Q. Document all disclosures of PHI and information related to such disclosures as would be required for DCH to respond to a request by an Individual or by the Secretary for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. By no later than fifteen (15) business days of receipt of a written request from DCH, or as otherwise required by state or federal law or regulation, or by another time as may be agreed upon in writing by the DCH HIPAA Privacy and Security Officer, Contractor shall provide an accounting of disclosures of PHI regarding an Individual to DCH. If requested by DCH, Contractor shall provide an accounting of disclosures directly to the individual. Contractor shall maintain a record of any accounting made directly to an individual at the individual's request and shall provide such record to the DCH upon request.

R. Work in good faith with DCH to promptly resolve any dispute, controversy or claim arising out of or relating to a violation of the HIPAA Privacy and Security Rules or Breach that arises from the conduct or omission of Business Associate or its employee(s), agent(s) or subcontractor(s). Business Associate acknowledges that such a violation of the HIPAA Privacy and Security Rules or breach of this Agreement may result in financial harm to DCH, including, but not limited to, damages, fines, civil penalties and reasonable attorneys' fees imposed on DCH as a result of such conduct or omission. Business Associate agrees to act in good faith to mitigate such financial harm to DCH, including, but not limited to, pursuing or assisting DCH in its pursuit of any financial recovery available through insurance or other financial coverage maintained by the Department of Administrative Services or any successor entity, pursuing any financial recovery available through Business Associate's contracts with

its agents or subcontractors as applicable, or taking such other action as determined reasonable by DCH and the Business Associate taking into consideration State budgetary requirements and restrictions.

9. DCH agrees that it will:

A. Notify Contractor of any new limitation in the applicable Notice of Privacy Practices in accordance with the provisions of the Privacy Rule if, and to the extent that, DCH determines in the exercise of its sole discretion that such limitation will affect Contractor's use or disclosure of PHI.

B. Notify Contractor of any change in, or revocation of, authorization by an Individual for DCH to use or disclose PHI to the extent that DCH determines in the exercise of its sole discretion that such change or revocation will affect Contractor's use or disclosure of PHI.

C. Notify Contractor of any restriction regarding its use or disclosure of PHI that DCH has agreed to in accordance with the Privacy Rule if, and to the extent that, DCH determines in the exercise of its sole discretion that such restriction will affect Contractor's use or disclosure of PHI.

D. Prior to agreeing to any changes in or revocation of permission by an Individual, or any restriction, to use or disclose PHI, DCH agrees to contact Contractor to determine feasibility of compliance. DCH agrees to assume all costs incurred by Contractor in compliance with such special requests.

10. The **Term of this Agreement** shall be effective on the Effective Date and shall terminate when all of the PHI provided by DCH to Contractor, or created or received by Contractor on behalf of DCH, is destroyed or returned to DCH, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this section.

A. Termination for Cause. Upon DCH's knowledge of a material breach of this Agreement by Contractor, DCH shall either:

i. Provide an opportunity for Contractor to cure the breach of Agreement within a reasonable period of time, which shall be within thirty (30) calendar days after receiving written notification of the breach by DCH;

ii. If Contractor fails to cure the breach of Agreement, terminate the Contract upon thirty (30) calendar days' notice; or

iii. If neither termination nor cure is feasible, DCH shall report the breach of Agreement to the Secretary of the Department of Health and Human Services.

B. Effect of Termination.

iv. Upon termination of this Agreement, for any reason, DCH and Contractor shall determine whether return of PHI is feasible. If return of the PHI is not feasible, Contractor agrees to continue to extend the protections of this Agreement to the PHI for so long as the Contractor maintains the PHI and shall limit the use and disclosure of the PHI to those purposes that made return or destruction of the PHI infeasible. If at any time it becomes feasible to return or destroy any such PHI maintained pursuant to this paragraph, Contractor must notify DCH and obtain instructions from DCH for either the return or destruction of the PHI.

v. Contractor agrees that it will limit its further use or disclosure of PHI only to those purposes DCH may, in the exercise of its sole discretion, deem to be in the public interest or necessary for the protection of such PHI, and will take such additional actions as DCH may require for the protection of patient privacy and the safeguarding, security and protection of such PHI.

vi. This Effect of Termination section survives the termination of the Agreement.

11. Interpretation. Any ambiguity in this Agreement shall be resolved to permit DCH and Contractor to comply with applicable laws, rules and regulations, the HIPAA Privacy Rule, the HIPAA Security Rule and any rules, regulations, requirements, rulings, interpretations, procedures or other actions related thereto that are promulgated, issued or taken by or on behalf of the Secretary; provided that applicable laws, rules and regulations and the laws of the State of Georgia shall supersede the Privacy Rule if, and to the extent that, they impose additional requirements, have requirements that are more stringent than or have been interpreted to provide greater protection of patient privacy or the security or safeguarding of PHI than those of the HIPAA Privacy Rule.

12. No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the Parties and the respective successors or assigns of the Parties, any rights, remedies, obligations or liabilities whatsoever.

13. All other terms and conditions contained in the Contract and any amendment thereto, not amended by this Agreement, shall remain in full force and effect.

(Signatures on following page)

IN WITNESS WHEREOF, Contractor, through its authorized officer and agent, has caused this Agreement to be executed on its behalf as of the date indicated.

GEORGIA DEPARTMENT OF PUBLIC HEALTH

ATTACHMENT B-1 - List of Individuals Permitted to Receive, Use, and Disclose DCH PHI

The following individual, as employees or agents of Contractor, need access to DCH Protected Health Information in order for Contractor to perform the services described in the Contract:

[Insert list of individuals with position titles]

Transfers of PHI must comply with DCH Policy and Procedure 419: Appropriate Use of Information Technology Resources.

Approved methods of secure delivery of PHI between Contractor and DCH:

- Secure FTP file transfer (preferred)
- Encrypted email or email sent through " secure tunnel' approved by DCH Information
- Security Officer
- Email of encrypted document (password must be sent by telephone only)
- Encrypted portable media device and tracked delivery method

Contractor must update this list as needed and provide the updated form to DCH. Use of DCH Protected Health Information by individuals who are not described on this Attachment B- 1, as amended from time to time, is impermissible and a violation of the Agreement. Contractor must update this Attachment B-1 as needed and provide the updated form to DCH.

DCH Project Leader Contact Information:

[Insert Project Leader for Medicaid and State Health Benefit Plan]

ATTACHMENT B-2 - List of Individuals Authorized to Access a DCH Information System Containing PHI

The following individuals, as employees or agents of Contractor, need access to DCH Information. Systems containing DCH Protected Health Information in order for Contractor to perform the services described in the Contract:

[Insert list of individuals with name of system and type of access]

The DCH Project Leader must submit a completed DCH Network Access Request Form for each individual listed above. Access will be granted and changed in accordance with DCH Policy and Procedure 435: Managing Authorization, Access and Control of Information Systems.

Contractor must notify the Project Leader identified in the Contract and the DCH Access Control Coordinator (dchois@dch.ga.gov and helpdesk@dch.ga.gov) immediately, but at least within 24 hours, after any individual on this list no longer needs the level of access described. Failure to provide this notification on time is a violation of the Agreement and will be reported as a security incident.

Contractor must update this **Attachment B-2** as needed and provide the updated form to DCH.

DCH Project Leader Contact Information:

[Insert Project Leader for Medicaid and State Health Benefit Plan]

ATTACHMENT C - Appropriate Use of Information Technology Resources Policy and Procedure

I. Purpose

The DCH Division of Information Technology seeks to promote the efficient use of information technology, and to promote the use of technology to deliver public services in a way that works better, costs less and is capable of serving our health plan members' and other customers' needs appropriately and effectively. The DCH Division of Information Technology also establishes DCH information security policy and procedures.

Information Technology (IT) Resources are provided to authorized individuals to facilitate the efficient and effective performance of their duties for the Georgia Department of Community Health (DCH). The IT Resources provided to individuals by DCH or at the request or direction of DCH, in order for those individuals to provide services for DCH, are referred to in this policy and procedure as "DCH IT Resources." Access to DCH IT Resources is limited in accordance with DCH Policy 435.

The purpose of this policy is to establish guidelines for the use of all DCH IT Resources, including those IT Resources managed by the Georgia Technology Authority and delivered by the State's IT Enterprise Service Providers - IBM and AT&T. These guidelines define appropriate business use of DCH IT Resources and establish requirements for protecting the privacy and security of electronic DCH information.

This policy also establishes required and appropriate information security controls that ensure the confidentiality, integrity and availability of DCH information and information systems and the privacy and security of DCH's electronic Protected Health Information.

II. Scope

This policy applies to all individuals who utilize, possess, or have access to DCH IT Resources in order to perform services for DCH as an employee or as a non- employee DCH worker "on assignment" with DCH (such as temporary staffing agency employees and independent contractors). These individuals are called "DCH IT Users" in this policy and procedure. See DCH Policy 435 for information about access to DCH IT Resources by other individuals pursuant to contractual agreements.

III. Definitions

“Documentt" refers to any kind of file that can be read on a computer screen as if it were a printed page, including files read in an Internet browser, any file meant to be accessed by a word processing or desk -top publishing program or its viewer, or the files prepared for reading by other software or other electronic publishing tools:

“Display" includes monitors, flat — panel active or passive matrix displays, LCD's, projectors, televisions and virtual -reality tools.

“Electronic media" means (1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or (2) Transmission media used to exchange information already in electronic storage media. Certain transmissions,

including paper via facsimile, and voice via telephone, are not considered to be transmissions via electronic media because the information being exchanged did not exist in electronic form before the transmission.

“Electronic protected health information" ("E- PHI” or **“ePHI")** means protected health information that is transmitted by electronic media or maintained in electronic media.

“Electronic mail" ("e-mail" or **"email")** is a method of composing, sending, storing, and receiving messages over electronic communication systems or Email Systems. The term email applies both to the Internet e-mail and to intranet systems allowing users within one agency or organization to send messages to each other.

“Email Systems" are software and hardware systems that transport messages from one computer user to another. E-mail systems range in scope and size from a local email system that carries messages to users within an agency or office to an e- mail system that sends and receives messages around the world over the Internet.

“E-mail messages" are electronic documents created and sent or received by a computer via an e-mail system. This definition applies equally to the contents of the communication, the transactional information, and any attachments associated with such communication. Email messages are similar to other forms of communicated messages, such as memoranda and letters.

“Encryption" means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

“GETS" means the Georgia Enterprise Technology Services IT privatization contract awarded by the Georgia Technology Authority to IBM and AT&T to provide consolidated IT Infrastructure and Network Management Services designed to ensure a stable, robust, secure, cost-effective, and centralized IT Platform and Service delivery model for the State of Georgia.

“Graphics" includes photographs, pictures, animations, movies, or drawings.

“Individually Identifiable Health Information" means information or data, including demographic information collected from an individual, that (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (3) That identifies the individual; or (4) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

“Information Technology Resources" or **"IT Resources"** means hardware, software, and communications equipment, including, but not limited to, personal computers, mainframes, networks, servers, portable computers, peripheral equipment, cell phones, personal digital assistants (PDA's), wireless communications, facsimile machines, technology facilities including but not limited to, data centers and dedicated training facilities and other relevant hardware and software items as well as personnel tasked with the implementation, and support of technology. The IT Resources provided to individuals

by DCH or at the request or direction of DCH, in order for those individuals to provide services for DCH, are referred to in this policy and procedure as "DCH IT Resources." All individuals who utilize, possess, or have access to DCH IT Resources in order to perform services for DCH as an employee or as a non-employee DCH worker "on assignment" with DCH (such as temporary staffing agency employees and independent contractors) are referred to as "DCH IT Users."

“Key Size" specifies the number of repetitions of transformation rounds that convert the input, called the plain text, into the final output called the cipher text.

“Limited Use" is defined as ten (10) minutes or less of personal use of the Internet during breaks or lunch.

“Protected Health Information" or **"PHI"** means Individually Identifiable Health Information that is (1) Transmitted by electronic media; (2) Maintained in electronic media; or (3) Transmitted or maintained in any other form or medium

“Removable Media" means portable USB -based memory sticks, also known as flash drives, thumb drives, jump drives, key drives, or writable and rewritable DVDs and CDs, and external hard drives.

IV. Policy

The DCH Division of Information Technology and its Office of Information Security shall ensure that GTA and the GETS Infrastructure and Network Management Service Providers take the appropriate steps, including the implementation of strongest -available and practicable encryption, user authentication, and virus protection measures, to mitigate risks to the privacy and security of DCH data and information systems associated with the use of DCH IT Resources by DCH IT Users.

DCH IT Users must protect DCH IT Resources from unauthorized access, misuse, and loss. DCH IT Users must protect the privacy and security of DCH IT Resources over which they have control or to which they have access. It is the responsibility of the User to manually lock their computer screen before leaving it unattended for any period of time. The DCH Division of Information Technology, Office of Information Security shall ensure that all DCH IT Users receive training necessary for them to protect the confidentiality, integrity, availability, privacy and security of the information over which they have control, or to which they have access, as a result of their use of DCH IT Resources. This training must be provided upon receipt of access to DCH IT Resources and on an as needed basis. In addition, this training must be provided on a regularly scheduled basis (annually or as close to annually as practicable).

V. Procedures

All DCH IT Users must satisfactorily complete initial Information Security Awareness Training and HIPAA Privacy/Security Training Programs and annual " refresher' training. Satisfactory completion of training will be demonstrated by the DCH IT Users providing correct answers to all quiz questions. Training materials and documentation of completion of training will be retained by the DCH Office of Human Resources for all DCH employees, and will be retained by the DCH HIPAA Privacy and Security Officer for all DCH IT Users who are not DCH employees. All DCH IT Users must comply with the provisions of this

policy and procedure, including the attached DCH Information Technology User Agreement, and any guidelines set forth in current training materials. Non- compliance with this policy and procedures, the attached DCH Information Technology User Agreement or guidelines set forth in current training materials will subject DCH IT Users to disciplinary action, up to and including termination, in accordance with applicable DCH Policies and Procedures, such as DCH Policy 911 (Sanctions).

DCH IT Users that become aware of any incident that threatens the privacy or security of DCH IT Resources should immediately report the existence of such incident to their immediate Supervisor, the Agency Information Security Officer (see Section XV for contact information), or in the case of security incidents involving PHI, the HIPAA Privacy and Security Officer (see Section XV for contact information).

Such incidents include, but are not limited to:

1) Loss, theft, or destruction of a DCH -issued desktop or laptop, regardless of whether the information is believed to be encrypted or otherwise safeguarded;

2) Loss, theft, or unintended destruction of any Media (including thumb drives, flash drives, CD' s, DVDs, external hard drives, etc.) that contains DCH information, regardless of whether the information stored in the Media is believed to be encrypted or otherwise safeguarded;

3) Loss, theft, or destruction of a DCH issued wireless or mobile device; including, but not limited to a BlackBerry, iPad, or other PDA, regardless of whether the information contained in the device is believed to be encrypted or otherwise safeguarded.

4) Fraudulent or unauthorized access to DCH information systems, including, but not limited to, those managed by GTA/GETS.

5) Sharing of passwords.

6) Improper use of GTA/GETS Managed e-mail services or Internet access.

7) Threats or damage to DCH employees, facilities, or systems.

DCH IT Resources are to be used only in a manner consistent with the goals and objectives of DCH, and are to be used to accomplish work-related assignments. DCH IT Users who divert DCH IT Resources for personal gain will be required to reimburse DCH and will be subject to other appropriate disciplinary action, including but not limited to termination.

Except as described below, DCH IT Users are not allowed to move any DCH IT Resource from its approved location. For example, the approved location for a DCH IT User's desktop computer is his ocher office or cubicle. The approved location for a printer, fax machine, or copier is the location approved by the DCH Support Services.

1) DCH IT Users may carry portable DCH IT Resources issued to them (such as DCH issued laptops, blackberries, iPads, or other PDAs) with them, as long as they maintain sole possession of these DCH IT Resources and secure them in

accordance with applicable DCH policies and procedures and guidelines from current training.

2) DCH IT Users may relocate other DCH IT Resources only with written approval of their Division, Office, section, or unit director and written approval of DCH Support Services or Division of Information Technology, whichever is responsible for issuing that type of DCH IT Resource.

3) DCH IT Users who work for GETS Service Providers, DCH Support Services, or in the Division of Information Technology may relocate DCH IT Resources as necessary to perform their work of issuing DCH IT Resources. They shall follow applicable internal procedures to ensure that all DCH IT Resources are inventoried and that access to DCH IT Resources is provided in accordance with the requirements of Policy 435.

4) DCH IT Users may not connect a personal flash drive, CD, DVD, or external hard drive to a DCH computer without written approval by a supervisor and the IT Department.

Guests may use their own portable media devices on their own computer or a loaner laptop provided by DCH IT but it should not be connected to the DCH network. If a guest needs internet access, DCH IT must set up an external internet connection.

VI. Software Licensing

The State's GETS Service Provider managed networks and Department Software Applications, and software are to be used responsibly by all DCH IT Users. DCH IT Users must comply with local, State, and federal laws related to copyrights, software licensing, and restrictions regarding the transmission of threatening or obscene materials. All computer software installed on DCH computers and systems must be licensed as required by the software manufacturer. All DCH IT Users must follow and abide by commercial licensing laws and requirements.

VII. Secure Password Standards

Passwords are essential in protecting State networks, systems, and sensitive agency data. Individual passwords are established and maintained by each employee for access to critical Information Technology business systems and software. Network, system, and application user accounts must be assigned to specific individuals and not assigned to anonymous user accounts, groups, departments, job functions, etc. DCH IT Users have a duty and responsibility to ensure that passwords remain private and confidential. Sharing LAN network, system, application, and/ or screen saver passwords with any other person is prohibited. Passwords prevent unauthorized access to various common directories on the network and the email system, as well as possibly access to external computer systems. DCH IT Users may give specific individuals access to their files and email by requesting such access through the Division of Information Technology. Strong Password Standards, as defined by State Enterprise Information Security Policies and Standards, must be followed for access to any State LAN network, system, or business software application.

Strong passwords include the following characteristics.

1) They must be at least eight characters in length; and

2) They must include three of the following four characters: and
   - English upper case (A -Z)
   - English lower case (a -z)
   - Numbers (0- 9)
   - Non -alpha special characters

3) They must not contain the user' s name; or

4) They must not contain part of the user's full name

VIII. Data Encryption Standards

All files, information or data containing ePHI shall be encrypted (utilizing the strongest available encryption technology and key size) while stored on removable Media and during transmission outside of DCH's network. DCH IT Users must follow the guidelines of current training materials regarding encryption of ePHI and methods for securely transmitting ePHI. Information and data containing ePHI shall also be encrypted before being backed -up to other data storage devices or Media. All ePHI data residing on DCH- issued desktop computers, portable computing devices (laptops) or other mobile computing devices shall be encrypted utilizing full -disk encryption technology. DCH IT Users shall not store any files or information containing ePHI to any removable Media, such as Flash Drives, CD's, DVD's, or external Hard Drives, etc. unless: (1) the DCH IT User' s supervisor has provided written approval for the DCH IT User to store the files or information on the removable Media, and 2) the DCH IT User saves the files to a DCH issued removable Media device, and (3) the information or data is encrypted while stored on the device. The encryption protocols utilized by DCH shall comply with the most current National Institute of Standards and Technology (NIST), FIPS- 197 Advanced Encryption Standard (AES).

DCH Division of Information Technology is responsible for ensuring encryption of ePHI "at rest" while stored on non- portable storage devices and backup storage devices to the extent practicable. As required by law, if encryption is not practicable, DCH Division of Information Technology shall maintain documentation of the reasons why encryption is not practicable as well as documentation that alternative physical, technical and administrative controls are being implemented to protect the privacy and security of the unencrypted ePHI. DCH IT Users are responsible for ensuring that ePHI is encrypted during transmission and during storage on portable Media devices. DCH IT Users should always utilize the strongest encryption protocol available when configuring wireless routers or networks at home.

IX. Saving ePHI

DCH IT Users shall save all files, information and data containing ePHI in a manner that restricts access to the ePHI to those who require access to it (either for current needs or for business continuity purposes), and that complies with applicable policies and procedures and current training guidelines.

Whenever possible, ePHI shall be saved to a DCH server, which is backed up, to prevent

inadvertent or unauthorized destruction.

All ePHI you save must be protected from access by others who do not need it. Documents and files containing ePHI that may be accessed by anyone in your Division must be saved in your Division folder on' the O:\Drive (or on your Division server). Only employees assigned to your Division may see files in your Division folder. Documents and files containing ePHI that may only be accessed by certain people in your Division must be saved in a restricted sub -folder in your Division folder (created by IT).

X. Malware and Anti -Virus Software

The GTA/GETS Infrastructure Service Provider has installed anti-virus software on the State network and information systems to detect and "sanitize" malware and virus programs that may be introduced. Accordingly, and for security reasons, the anti-virus software programs must not be disabled. Downloading and installing software from outside the office or from the Internet on State desktop or laptop hard drives without written approval from the Division of Information Technology is strictly prohibited. This is necessary due to the limited availability of hard disk space, the danger of importing computer SPAM and viruses, and the software licensing issues mentioned above. These SPAM e-mails can redirect a user's Web Browser to virus infected Web Sites which can install malicious software on State computers and networks. However, these devices cannot block all e- mails containing such Links. DCH IT Users should never click on Web Links in e- mails from unknown or suspicious sources. When in doubt, contact the Division of Information Technology Help Desk or the Agency Information Security Officer.

Virus protection must be running on your computers. Always restart your machine to pick up the latest patches and virus definitions. NEVER open any files attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then “double delete" them by emptying your Trash. Delete spam, chain, and other junk email without forwarding. Do not download files from websites unless absolutely necessary to accomplish your work. Never download freeware onto your workstation. If your computer detects a virus, stop using the computer and notify the DCH IT Help Desk or call the GETS help desk at 877-482-3233 immediately.

Personal information technology resources may never be connected to DCH IT Resources. DCH Management reserves the right to examine and review content on personal information technology resources reasonably believed to have been connected to DCH IT Resources or to contain DCH information. Examples include but are not limited to items such as personal USB drives, personal external hard drives, personal CD's, DVDs, personal laptops or any other personal computing device that has the ability to connect with DCH Information Technology Resources.

XI. Internet and E- mail Use

Personal

The State's Infrastructure Service Providers provide Internet access and e- mail addresses as required by DCH to DCH IT Users for the efficient and effective performance of their duties for DCH. Internet access is provided to allow business-related research and access to information needed to facilitate business communication with customers, vendors, colleagues and others receiving services from, doing business with, or seeking

information from DCH. Computer equipment and other IT Resources required for Internet access. And email accounts are provided at significant cost to the State, and as with other State property, DCH IT Users must ensure that such resources are not misused. Although valuable business tools, Internet and e-mail access are considered privileges, and as such DCH reserves the right to revoke access to either or both for inappropriate usage or take any other appropriate disciplinary action, including termination.

Examples of inappropriate Internet use include, but are not limited to, the following:

1) Private or personal for-profit business activities. This includes Internet use for private purposes such as private advertising of products or services, or any activity meant to foster personal gain.

2) For profit business transactions or unauthorized not-for-profit business activities.

3) Conducting any illegal activities as defined by federal, State, and local laws or regulations.

4) Political or religious causes.

5) Accessing or downloading sexually explicit or pornographic material.

6) Accessing or downloading material that could be considered discriminatory, offensive, threatening, harassing, or intimidating, including ethnic or racial slurs or jokes.

7) Gambling.

8) Uploading or downloading commercial or agency software in violation of copyright or trademark.

9) Downloading any software or electronic files without approval from the IT Division or ensuring that DCH provided virus protection is active.

10) On-line shopping and auctioning.

11) Accessing Web chat sites and dating sites.

Examples of appropriate Internet use include the following:

1) Job- related research.

2) Access to federal, State, or local government Internet sites.

3) Access to sites related to professional organizations or other professional development information.

4) Limited use during personal time (i.e., breaks and lunch).

Information, data and files composed, transmitted, or received on DCH IT Resources, including Internet data and e-mail messages, are subject to disclosure under the Georgia Public Records Act:

DCH IT Users should ensure that all data accessed with or stored on DCH IT Resources is appropriate, ethical and lawful. E-mail users should be mindful of how they represent themselves, since any message or data sent through the e- mail system clearly identifies the message as coming from DCH and could be interpreted as a Statement of DCH opinion, position or policy. Additionally, data that is composed, transmitted, accessed or received via State Internet resources must not contain content that may be considered discriminatory, offensive, threatening, harassing, intimidating, or disruptive.

Email is NOT the same as a letter sent through the normal mail: Your messages are written" on the electronic equivalent of postcards. What does this means? Anyone can look at your message. Do not email ePHI to a non -DCH email account, unless the email has been encrypted. If you need to email ePHI to perform your job, please use Voltage ("Send Secure") encryption or contact your local support team for instruction. Do not use non–DCH email such as Web Mail (like gmail, hotmail, yahoo, etc.) to conduct business or send ePHI. Secure FTP (SFTP) may be used to send ePHI outside of DCH. Contact the IT Help Desk for instructions.

Before you send an Email that contains PHI: check all addresses for accuracy, use "Send Secure", and consider using an Email delay feature that allows you to stop an Email from going out if you accidentally hit "Send" instead of "Send Secure". MOVE Emails that contain attachments with PHI to folders on your P: Drive. Sending ePHI Out of DCH.SECURE FTP File Transfer Protocol) is the BEST way to exchange large files containing ePHI. If you regularly need to get or send a large file containing ePHI outside the DCH network, contact the IT Department to set up Secure FTP (SFTP). "Send Secure" email may be used to send smaller files. Send Secure will encrypt the message and the file. If Send Secure is not available, you may email a message that does not contain ePHI and attach an encrypted file. Excel, Access, Word, PDF all have instructions for encrypting the document. Encryption is different from "password protection". It is YOUR responsibility to ask the ISO if you do not know how to encrypt a file. The password to open the encrypted file must be a strong password and must be sent using "Send Secure" email or shared by phone, fax or mail. If you regularly need to email ePHI to a vendor, contact the ISO to make sure that DCH has a secure, encrypted "tunnel" to the vendor. If a secure tunnel exists, "Send Secure" is not necessary, but is still the best choice. Always email to the vendor contact's work email. The secure tunnel only works between your DCH email address and the vendor's work email address. It is ok to email ePHI to a DCH worker at the DCH email address if necessary. Only email the minimum necessary ePHI. Only include authorized individuals on the email. Review any email before forwarding to make sure you are not sending ePHI to someone who does not have a need to see it. Any large file containing ePHI should be saved in a Restricted Folder. Email the path to the folder instead of the file itself. Never send ePHI to any personal email -address without supervisor approval. ePHI may only be sent for business purposes. Email is usually not a good way communicate ePHI to customers. All email must contain the following statement: Reader Advisory Notice: Email to and from a Georgia state agency is generally public record, except for content that is confidential under specific laws. Security by encryption is applied to all confidential information sent by email from the Georgia Department of Community Health.

XII. Monitoring Use of DCH IT Resources

While DCH respects the privacy of DCHIT Users, ensuring compliance with this policy and procedure is of utmost importance. Therefore, DCH reserves the right to retrieve and read

content or data including but not limited to any data composed on DCH IT Resources, transmitted using DCH IT Resources, received through DCH on- line connections, or stored on DCH IT Resources, to monitor Internet sites visited and access attempts, and provide information relevant to an investigation of suspected violations of DCH policies and procedures or laws. Inappropriate Internet or e-mail usage can expose DCH to significant legal liability and reflect negatively on DCH. The State's Infrastructure Service Provider has installed software to prevent access to many objectionable Internet Web content and to monitor State Internet access.

The Division of Information Technology may review and document Internet activity, email usage or usage of other DCH IT Resources. DCH IT Users should be aware that any information accessed, downloaded, or transmitted may be reviewed by information security staff, the Office of Inspector General, and the HIPAA Privacy and Security Officer, as needed, and DCH management will be notified if a DCH IT User's use of DCH IT Resources violates DCH policies or procedures or laws, such as by repeatedly attempting to reach blocked Internet sites, frequently visiting non -work related sites, or emailing DCH information to personal email accounts. When using DCH IT Resources, including, but not limited to e-mail and Internet, DCH IT Users are consenting to the monitoring of their use and have no reasonable expectation of privacy in the use of the DCH IT Resources. Failure to comply with this policy and procedure may result in disciplinary action, up to and including termination from employment.

XIII. Policy and Procedure Revisions

The Chief Information Officer (or his designee) is responsible for reviewing, maintaining and updating this policy and procedure, the attached DCH Information Technology User Agreement, and Information Security training materials as necessary and appropriate.

XIV. Dissemination

This policy and its attachments must be reviewed and acknowledged by all DCH IT Users during Orientation or upon being provided with access DCH IT Resources, whichever comes first. In addition, the policy will be posted on the DCH Intranet Web Portal and made available to all DCH IT Users. Any revisions to the policy and its attachments will be communicated to all DCH IT Users and knowledge of the policies and procedures must be acknowledged, in writing, by all DCH IT Users at least annually.

XV. Information Security and HIPAA Privacy and Security Contacts

Agency Information Security Officer

Agency HIPAA Privacy & Security Officer

Division of Information Technology Help Desk

Appendix A - Information Technology User Agreement

By accessing DCH IT Resources, DCH IT Users agree to maintain the privacy, security, confidentiality and integrity of State and DCH data and computing resources over which he or she has control or to which he or she may have access. DCH IT Users must review this policy and procedure and the current Information Security Training materials and agree to comply with them by signing the DCH Policies and Procedures Acknowledgement Form upon start of work and annually thereafter.

Use of Information Technology Resources

1) DCH IT Users shall not attempt to circumvent IT privacy or security safeguards, and any such attempts may lead to revocation of a DCH IT User's access and may result in disciplinary action, as appropriate.

2) DCH IT Resources, including e- mail accounts and Internet access, may be monitored at any time without additional prior notice, and if such monitoring reveals violations of State or DCH policies, the Chief Information Officer (CIO) or his designee and the Office of Human. Resources will be notified and appropriate sanctions will be applied. If such monitoring reveals misconduct or illegal behavior, the activity will be referred to the DCH Office of Inspector General for internal investigation and further action, as needed.

3) DCH IT Users shall not add any network equipment or infrastructure to the State network except as authorized by Division of Information Technology or GTA/GETS Service Provider management as part of a DCH IT User's job responsibilities. The DCH IT User's supervisor or contracted business program sponsor must inform the Division of Information Technology when he or she no longer requires access to DCH IT Resources, in accordance with DCH Policy 435.

4) DCH IT Users shall not relocate computing equipment, workstations, printers, scanners, etc., without proper authorization or assistance from the appropriate Division of Information Technology support staff.

5) DCH IT Users shall only physically connect to the State's Infrastructure network using DCH IT Resources.

6) DCH IT Users shall not disclose ePHI in e-mail unless the e- mail is encrypted as described in current training guidelines.

7) DCH IT Users shall use their best efforts to send only e- mail content that is appropriate for transmission in that media, ensuring messages are professional, current, accurate, and factual.

8) DCH IT Users will be mindful of the right of any person to inspect and copy emails upon request, under the State of Georgia public records law.

9) DCH IT Users shall take reasonable and appropriate steps to protect DCH IT Resources from loss, damage, or theft and understands that failure to do so may result in disciplinary action.

10) DCH IT Users shall not attempt to introduce a computer virus or other malicious program code into State networks, systems, or software.

11) DCH IT Users shall not attempt to bypass, strain, or test security safeguards or mechanisms, unless authorized as required by specific job responsibilities.

12) DCH IT Users shall comply with guidelines set forth in current Information Privacy and Security training materials.

Software Licensing and Intellectual Property

DCH IT Users requiring additional computer software, equipment, or media that was not originally issued, shall contact the Division of Information Technology Help Desk to request the required resources. The Division of Information Technology will ensure that the appropriate software licensing and agreements are obtained. DCH IT Users shall not download, use or connect any unauthorized software, freeware, adware, shareware; or hardware onto any State network, system, workstation, wireless/mobile device, nor violate software copyright, trademark or licensing restrictions.

ATTACHMENT D - Technology & Security Standards Policy and Procedure

I. Purpose

A. Provide the general framework of the policy and procedure utilized by the Department of Community Health (DCH) to control access to information and associated applications governing agency operations;

B. Clearly document information access control policy and procedures;

C. Avoid the negative consequences that result when information systems are compromised, which consequences may include:

(1) Sanctions;

(2) Negative media attention;

(3) Exposure of personal or private information and subsequent harm to individuals; and

(4) Unauthorized access to DCH's applications including unauthorized viewing, modifications, and copying of data.

D. Provide for the development of access controls required to protect state and federal information systems.

E. Mitigate the risk of threats or incidents involving current or former employees or contractors who intentionally exceed or misuse an authorized level of access to a network or system or access data in a manner that affects the security of DCH data, systems or daily business operations.

F. Outline managers' responsibilities and role in managing authorization, access to and control of DCH's systems and applications as outlined specifically and agreed to in DCH Information Technology User Agreement.

G. Establish access control requirements for DCH contractors and business owners, as well as vendors, sponsors, and partners, in regards to their role and responsibilities, when access to DCH data and/or use of applications associated with DCH operations is authorized.

(1) Reinforce the role of the business owner in providing adequate oversight of contractors' responsibilities specific to access control outlined in DCH contracts.

(2) Ensure that valid business needs for access associated with DCH assignments continue to exist and that those needs are periodically reviewed and evaluated.

(3) Assure compliance with all laws that require access controls procedures, including those identified as "References" in the header at the beginning of this document.

II. Policy

A. DCH information shall be used solely for appropriate agency purposes so that reasonable efforts are made to prevent any use or disclosure of Protected Health Information (PHI) in violation of HIPAA.

(1) DCH information shall not be accessed by or disclosed to anyone who does not need the information to perform the activities and fulfill the responsibilities associated with his or her role as stated in Policy 419: DCH IT Use of State Computers

(2) Those authorized to grant or revoke access to DCH information are responsible for following applicable procedures to ensure that access is appropriately assigned, modified as needed, and canceled promptly when individuals transfer to other positions or leave DCH.

(3) Those accepting confidential information on behalf of DCH shall ensure that the requirements related to the acceptance of that information are followed.

(4) Addressing the misuse of Department information and violations of IT Policy 419 is of paramount importance to DCH and will be dealt with on a priority basis. Alleged violations of this policy will be investigated in accordance with the appropriate legal requirements and DCH disciplinary procedures, and when appropriate, sanctions, including, but not limited to, dismissal, will be imposed.

B. Unless specifically designated as a public information system, access to any DCH information system network and its resources shall require the use of identification and authentication credentials in accordance with Policy 419 and the terms of applicable contracts.

C. All contracts that involve access to DCH systems shall include the requirement that DCH's IT Division be notified (in accordance with DCH instructions) immediately (and, in no event, more than 1 business day) after any modification or termination of roles. This applies to all DCH business owners, contractors, and vendors.

D. Access authorization shall follow the guidelines established by this policy and procedure.

E. Access authorization shall be documented, monitored and managed in accordance with state and DCH guidelines.

F. DCH deploys Role Based Access control measures which are based on an individual's role and responsibilities with DCH.

G. Roles are assigned by the Supervisor/Manager based on an employee's function within the organization.

H. Supervisors/ Managers are responsible for validating and communicating roles and access, where the level of access to be authorized is the lowest level required for users to meet their DCH responsibilities.

I. Upon termination of employment or reassignment of job responsibilities, an employee's user ids and password shall be deleted in accordance with the DCH Enterprise Security policy.

J. Upon re -assignment of job responsibilities, an employee's access privileges shall be changed accordingly.

III. Scope

A. This policy establishes requirements for individuals regarding access to all DCH information, including the responsibilities of stewardship and accountability for DCH information needed in carrying out DCH's mission and/ or conducting DCH business.

B. This policy refers to information systems that are used by DCH'. Access control is required in order to comply with federal and state regulations and to safeguard the confidentiality, integrity and availability of sensitive and confidential information, including PHI.

C. This policy describes those procedures necessary for requesting, modifying and deleting user access to systems, applications and data covered by federal, state and all other applicable rules and regulations.

D. This policy applies to all who have access to DCH systems but whose access is not specified in a Business Associate Agreement or a Data Use Agreement.

IV. Roles and Responsibilities

A. Georgia Technology Authority (GTA): GTA manages access to the State's technology infrastructure and network services. GTA also controls some applications used by DCH. In addition, GTA manages administrative and physical access to systems. GTA is responsible for all matters related to the State's contracting with outside parties for GETS functions.

B. Georgia Building Authority (GBA) manages the office space occupied by DCH and provides the physical security necessary to provide a secure environment for people, equipment and information. GBA also manages the Building Access Request System, and physical access to the building.

C. DCH Offices, Management, and Staff

1. Commissioner

a) Leads DCH and conveys the importance of information security to DCH management and staff.

b) Supervises the CIO and communicates with other State leaders and the Governor's Office to promote efficient and effective information security measures. The Commissioner has the final authority regarding the granting or termination of information access rights.

2. Chief Information Officer (CIO)

a) Designates a senior agency information security officer (SAISO) who shall carry out the CIO's responsibilities for information security access control planning and implementation.

b) Provides guidance and oversight regarding all DCH information security policies, procedures, and access control safeguards to address identity and access management.

c) Oversees the identification, implementation, and assessment of security access controls throughout DCH's Technology Enterprise.

d) Ensures that personnel with responsibilities for system, network, and application security access controls are appropriately trained.

e) Assists other senior DCH management with their responsibilities for system, network, and application access security.

f) Oversees the coordination of cross -platform security access controls for DCH.

g) Collaborates with the Executive Director of GTA and other State CIO's to address technology and security issues, policies, and standards.

3. Information Security Officer [in the Office of Information Technology (OIT)]

a) Manages information security access control planning and implementation on behalf of the CIO.

b) Coordinates the development, review, and acceptance of security access controls with IT system owners, access security administration staff, and business owners or authorizing officials.

c) Coordinates the identification, implementation, and assessment of network, system, and application access security controls.

d) Plays an active role in developing and updating security access control policies, procedures, and standards and assesses the security impact.

e) Collaborates with the State Chief Information Security Officer and other State agency Information Security Officers to address Enterprise Security Access Control Policies, Procedures, and Standards and their impact on DCH business operations.

f) Provides oversight and guidance to security administration and operations staff regarding security access control policies, procedures, and standards.

4. Access Control Coordinator/Systems Administrator

a) Sets and administers system -wide security controls appropriate for the authority given to users in accordance with the attributes or privileges associated with access control systems.

b) Acts as the first step of security by creating user ids and passwords to access the local file servers.

c) Is appointed by CIO as the owner and manages the authorized access list.

d) Acts as the primary point of contact to control settings and coordinate administrative changes for statewide applications, including assigning permission for certain functions and access levels.

5. Inspector General

   a) Oversees the criminal background check process for all DCH employees.

   b) Coordinates with Director of Human Resources to ensure proper background checks for independent contractors and temporary staffing agency employees are complete before access to information systems is granted.

   c) Directs investigations related to violations of DCH information security procedures, including access control procedures, and works with the HIPAA Privacy and Security Officer to recommend sanctions.

   d) Coordinates with the Attorney General and law enforcement when any information security incidents involve criminal behavior.

6. Chief Financial Officer (CFO)

   The CFO is the primary authority for access by DCH staff to the PeopleSoft Financial System and related data. The CFO must approve the level of access to the Financial Systems before user ids and passwords are created.

7. Contracts Administration

   a) Is responsible for ensuring that all contracts with business entities that have access to DCH information systems, or that operate information systems on behalf of DCH, includes provisions requiring the maintenance and implementation of acceptable information security controls, including access controls.

   b) Ensures that such contracts incorporate access controls related to DCH information systems and provide penalties for failure to promptly inform DCH of a need for access changes.

8. HIPAA Privacy and Security Officer

   a) Works with the CIO, Information Security Officer and Commissioner to revise DCH security controls as needed and ensure proper documentation in DCH policies and procedures.

   b) Works with the CIO, Information Security Officer and Director of Communications to promote compliance with HIPAA security regulations and ensure that all DCH workforce members receive regular security awareness training, including training on access controls.

   c) Works with the Director of Contracts Administration to clarify roles and responsibilities regarding HIPAA security compliance: by business associates and develop contract language to address access controls.

d) Works with the Director of Support Services to promote physical access controls, including physical security of information systems through worksite audits and support of secure document storage/destruction practices.

e) Works with the Inspector General to investigate violations of DCH information security procedures and recommends sanctions for such violations.

9. Office of Human Resources

a) Is responsible for ensuring that DCH maintains documentation showing that all independent contractors and temporary staffing agency workers have been properly screened in accordance with policies and procedures for background checks.

b) Maintains documentation that each member of the DCH workforce has access only to those information systems necessary to perform his/her work.

c) Ensures that all new members of the DCH workforce receive HIPAA Privacy and Security training, which includes training on access restrictions, before receiving access to DCH information systems.

d) Ensures that all new members of the DCH workforce sign an acknowledgment of the DCH information security procedures.

e) Maintains HIPAA training and acknowledgment forms for DCH employees, and ensures that such forms are provided to the HIPAA Privacy and Security Officer for all independent contractors and temporary staffing agency workers.

f) Ensures that all supervisors are aware of their responsibility to approve information system access only as needed and change the access whenever a staff member's access requirements change.

g) Ensures that the process for termination of employment includes termination of access to information systems.

10. Support Services

a) Coordinates with GBA and GTA to ensure that physical access to DCH workspace and information systems storage is properly limited through badge access and other controls.

b) Works with law enforcement to notify DCH staff members of threats to information system arising from break-ins and thefts.

c) Coordinates with DCH and other State leaders to ensure that business continuity plans are current and appropriate.

d) Supports security breach investigations.

11. Director of Vendor and Grantee Management

a) Monitors compliance by vendors with information security provisions in service level agreements, including provisions related to access controls.

b) Is responsible for including information security audits in the vendor management audit process.

12. Director of Procurement/Agency Procurement Officer (APO)

    The Director of Procurement/APO is the primary authority for access to the PeopleSoft Team Georgia Marketplace (TGM) data by DCH staff. The APO must approve the level of access to the TGM system before a user ID and password is created for the employee.

13. System Administrators

    a) Are uniquely responsible for enabling users to manage a system or server.

    b) When appropriate, authorize users to define or alter user ids, set security controls on a system or alter system components. These higher level privileges are restricted and controlled and may be extended to performing system support and maintenance activities if not assigned at the enterprise level.

    c) Authorize and manage users' access to systems (as listed in the Request for Network Access Form) with privileges defined by job function and role within DCH.

    d) Serve as the primary business owners for the application/ platform system with authorization to perform job functions.

    e) Validate privileges annually and report updates to DCH Access Control Coordinator, and perform requested changes to DCH premium networks after ensuring that proper authorization has been obtained.

    f) Retain revalidation results, evidence of completion and supporting communications for at least 6 years per HIPPA requirements, and define and manage access control requirements, including authorization processes and user ID and password rules for managed applications and systems.

    g) Maintain event/activity logs on all actions for each, application under their control.

    h) Are primarily responsible for access to all DCH data closets. Entry for any other staff is strictly prohibited unless an emergency (e. g., fire or water damage) dictates otherwise.

14. Individual Users

    a) Defined as any user or network member that requires access to any network, system, or application that accesses, transmits, receives, or stores electronic information.

    b) User ids for DCH applications shall not be shared and individual accountability for security of those ids must be maintained.

c) Authorized users are responsible for keeping all account authentication information in a secure place and not permitting any other person to use such accounts for any purpose.

d) Authorized users shall use all necessary precautions to safeguard confidentiality of associated passwords and shall change passwords when directed to comply with scheduled security reviews.

e) Authorized users shall notify the CIO immediately if their password is compromised and is shall not use a password belonging to someone else.

f) The user is accountable for all activity performed using applicable ids.

g) Authorized users acknowledge that when they are no longer employees of DCH, authorization to use the account will be terminated.

D. State of Georgia recognizes three (3) types of user accounts: Service Account, User Account and Privileged Account. [Service Accounts can be privileged, if technically required, but User Accounts may not. All User Accounts should have a named owner and follow the password policies of the State

1. Service Account - Service Accounts are used to allow system services or applications to connect to a system. These accounts are not intended for individuals to use interactively.

2. User Account - User Accounts are designed for use by general users with non-privileged system access.

3. Privileged Account - Privileged Accounts enable a user to manage a system or server. They may allow a user to define or alter user ids, set the security controls on the system or alter system components. Access to Privileged Accounts is not granted to the general user and should be restricted and controlled.

V. Procedure

A. Manager/Supervisor/Business Owner shall:

1. Complete a Request for Network Access form (see Attachment A) to identify an individual DCH user who requires access to the DCH computer system/ application. This form is required for access request initiation, updates, and terminations.

2. Scan and send the completed form electronically to the DCH Access Coordinator. Print and sign in the Manager Approval section to indicate approval for the access requested.

3. Keep the form in a secure, on- site location (e.g., the users personnel file held by the Manager/Supervisor), readily available upon request.

4. Review the assignment of computer systems annually for employees under his/her direct supervision to ensure that business need still exists for the specific application.

5. Review access as users change positions or work assignments (e.g., promotion, demotion, transfer, role change, extended leave or rehire) to ensure that access is maintained or revoked, as appropriate.

B. Access Coordinator/Agency System Administrator shall:

1. Grant access as specified on the Network Access form and notify the manager/supervisor/business owner when complete.

2. Forward requests for specific applications to the designated system administrator.

3. Modify or revoke access privileges when users are operating outside their work assignments.

4. Revoke access privileges during a user's extended leave or when deemed appropriate by the Human Resources Office.

5. Request appropriate modification or termination of access privileges to information assets and data systems in accordance with the following:

    a) When the user terminates employment with DCH or the need for access no longer exists, access shall be terminated.

    b) After 60- 90 days of no logon to information systems or applications, access shall be terminated.

    c) When there is unauthorized or wrongful use or disclosure of information, access shall be terminated in accordance with DCH Enterprise Security Policy.

    d) Upon completion of a projector contract work, access shall be terminated and the application administrator shall be notified. A Request for Network Access Form must be submitted before access can be reinstated.

C. Access to Functions

1. Users shall be granted access only to the extent necessary to perform their functions at DCH. Access can be restricted to specific functions within some applications. Whenever the software allows, access should be as specific and limited as feasible. Users should only have read or write access to the specific ePHI data required for performing their appropriate function. In most cases, access will fall into one of the following categories:

    a) Administrator/Super-User; or

    b) Regular or Normal User Accounts

2. The minimum access control requirement is a username and strong password. Every user at DCH must have a unique username. User names shall not be shared. For more information on this policy, see IT Policy 419.

    a) Role -based access may be employed where it improves specificity of access. Role - based access allows end- users to access information and resources

based on their role within the organization. Role -based access can apply to job categories or to groups of people or individuals.

b) The use of Anonymous accounts violates this policy and is strictly prohibited. The use of anonymous user accounts that are able to access internal agency IT resources, including, but not limited to, PHI, is strictly prohibited unless specifically authorized in writing by the CIO.

3. If approved by the DCH Information Security Officer and the HIPAA Privacy and Security Officer, DCH may create user accounts for an entity other than DCH that are, in turn, authorized to create, modify and terminate sub -accounts. The security privileges of the user accounts must be approved by the DCH ISO and the HIPAA Privacy and Security Officer. The entities for which the user accounts are created must enter into a written agreement with DCH that describes both the security privileges and the proper use of the accounts. Each such agreement shall set out in specificity the requirements the entity shall follow, which procedures shall be similar to those established by Policy 435, and to maintain at all times Network Access Control forms approved by DCH which are substantially similar to the one attached to this Policy 435. The agreement shall include penalties or other appropriate consequences, as permitted by law, for failure to promptly terminate access, and shall require the entities to file quarterly updates showing the current users and. affirming that their continued use and level of access continue to be appropriate or should be modified.

D. Eligibility for Access

1. Employees whose job responsibilities require access to PHI maybe authorized to access specific applications which provide access to PHI, if appropriate, with the written approval of the System Owner and the HIPAA Privacy and Security Officer.

2. Contractors/Temporary Staff providing support to specific DCH functions on a time-limited basis may be authorized access to specific applications for the duration of their assignments with the written approval of the System Owner.

3. Access shall only be granted to users whose status with DCH is current.

4. Whenever job responsibilities change, the supervisor shall review and determine the appropriate access and request the corresponding changes by using the Request for Network Access Form.

5. If an individual no longer requires access (e.g., upon termination of employment) all access shall be terminated immediately.

E. Access Determination

1. Determining the access to specific applications necessary for job functions and responsibilities requires determining which applications are required based on those functions and the corresponding data needed.

2. Every user should be granted the lowest level of access necessary to meet his/ her DCH job responsibilities. This practice is intended to limit the damage that could result from accidents or errors.

F. Monitoring and Oversight

1. The Information Security Officer shall conduct periodic reviews to validate the appropriateness of user accounts and access privileges.

2. Supervisors and System Administrators shall review access requirements annually.

3. Supervisors shall review user access at least twice per year, which reviews can be accomplished during an employee's midyear and annual performance reviews to ensure that each user's access is appropriate.

4. System administrators shall review all user access periodically as a critical function of his/her responsibility to ensure that all users are in current status.

5. All system users consent to such monitoring and accept responsibility to preserve the confidentiality, integrity, and availability of information accessed.

G. Training and Access

1. All DCH employees shall complete HIPAA security training during their new hire orientation and during refresher training as designated by the HIPAA Privacy and Security Officer.

2. Regularly scheduled system activity reviews shall be conducted by System Administrators to ensure that the level of access to the system is appropriate.

VI. Supporting Documentation

Software	Required Documentation
PeopleSoft 8.9 HCM Security	Upon approval application is faxed to State Accounting Office, 200 Piedmont Avenue, Suite 1602 West Tower, and Atlanta, GA 30334. Fax # 404-463-5089.
HRM Query Access Request	Upon approval application is faxed to HRMS Phoenix Security, 200 Piedmont Avenue, Suite 1602 West Tower, and Atlanta, GA 30334. Fax # 404- 651- 5113.
PeopleSoft FN Financial 9. 0	Forms can be faxed to 404-463-5089 Attn: Security or mail forms to: State Accounting Office, 200 Piedmont Avenue, Suite 1602 West Tower, Atlanta, GA 30334, Attention: Security.

VII. Glossary of Terms

Term	Definition
Access Control Coordinator	The authority given to an individual by the assignment of attributes or privileges that are associated with access control systems and that are required for setting and administering system -wide security controls. Individual is designated by the Chief Operating Officer.
Administrator/Super-User	A special user account used for system administration. Depending on the operating system, the actual name of this account might be: root, administrator or supervisor.

Term	Definition
Agency Procurement Officer (APO)	Primary authority for access to the PeopleSoft Team Georgia Marketplace (TGM) data by DCH staff.
Contractor	An organization or individual that contracts with the Department to supply needed service, or skill set.
Georgia Building Authority (GBA)	The State Authority that manages the property occupied by State agencies and provides the physical security necessary to provide a secure environment for people, equipment and information.
Georgia Technology Authority (GTA)	The State Authority that establishes information security standards and requirements for the State of Georgia.
HIPAA	Health Insurance Portability and Accountability Act, a US law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers.
IT Sabotage	Cases in which current or former employees or contractors intentionally exceed or misuse an authorized level of access to networks, systems, or data with the intention of harming a specific individual, the agency, the agency' s data, systems, and/ or daily operations.
Privileged Account	Accounts that enable a user to manage a system or server.
Protected. Health Information (PHI)	Protected health information is defined in 45 CFR 160. 103, means individually identifiable health information that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium.
Resource Access control Facility (RACF)	Designed to provide improved security and controls what users can do on the operating system.
Role Based Access (RBAC)	An approach to restricting system access to authorized, users. The primary rule for RBAC is as follows: Role assignment and authorization: A user shall be granted system access based on his/her assigned and authorized active role in DCH.
Security Planning	Requires organizations to have security controls in place or planned for their information systems and the rules of behavior for individuals accessing the information systems.
Service Account	Used to allow system services or applications to connect to a platform resource.
Theft Of Information	Cases in which current or former employees or contractors intentionally exceed or misuse an authorized level of access to networks, systems or data with the intention of stealing or modifying confidential or proprietary information for the organization.
Third Parties	Parties who contract with the DCH that administer applications, on the agency's behalf, that are covered by HIPAA security regulations or that represent significant financial risk to the DCH.
User Account	Defined as general users with non -privileged system access.

VIII. Version Control [removed]