TABLE OF CONTENTS

HIPAA POLICIES:

General HIPAA Compliance and Enforcement

Topic: HIPAA Compliance

Date Adopted: 3/17/2020

I. POLICY

Deborah Cardiovascular Group, P.C. ("DCG") recognizes its obligation to comply with the Health Insurance Portability and Accountability Act ("HIPAA") as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH") and their implementing rules and regulations, as well as applicable State licensing and other laws requiring the protection of the confidentiality, integrity and availability of patient records and information. DCG implements and maintains a HIPAA Compliance Program in order to comply with HIPAA, HITECH and applicable state and federal privacy and related laws and regulations.

II. DEFINITIONS

1. Individually Identifiable Health Information - *Individually identifiable health information* (IIHI) is information that is a subset of health information, including demographic information collected from an individual, and
    a) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
    b) 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
        i. That identifies the individual; or
        ii. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
2. Protected Health Information – *Protected Health Information* (PHI) is IIHI that is transmitted or maintained in electronic media, or transmitted or maintained in any other form or medium. PHI does not include:
    a) IIHI in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
    b) IIHI in records described at 20 U.S.C. 1232g(a)(4)(B)(iv);

c) IIHI in employment records held by a covered entity in its role as an employer; and

d) Regarding a person who has been deceased for more than 50 years.

III. PROCEDURES

1. HIPAA Compliance and Security Officers. DCG shall formally designate and maintain the positions of **HIPAA Privacy Officer** and **HIPAA Security Officer** who shall be responsible for all HIPAA privacy and security compliance by DCG. The positions of Privacy Officer and HIPAA Security Officer may be jointly held by one individual, at DCG's discretion. Such Officers shall be responsible for the general oversight, implementation and enforcement of the HIPAA Compliance Program and shall perform their job responsibilities as set forth in DCG Policy "Assigned HIPAA Responsibility" and "Assigned Security Responsibility".

2. Privacy & Security Policies. DCG shall develop, implement, maintain and periodically update such policies and procedures necessary for DCG to comply with its privacy and security obligations under HIPAA as well as any related obligations under federal and state law that are appropriate to DCG's size, capabilities, complexities, the nature of its operations, technical infrastructure, hardware, and software capabilities, and anticipated or actual risks to PHI that it may create, receive, maintain or transmit (the "P&S Policies").

3. HIPAA Committees. DCG shall designate, as appropriate, HIPAA Committees responsible for governance and oversight of the HIPAA Compliance Program. The HIPAA Committees shall oversee and enforce the HIPAA Compliance Program together with the HIPAA Security Officer and HIPAA Privacy Officer.

4. Training. DCG shall develop and implement training for all workforce members on the HIPAA Compliance Program in accordance with DCG's "Training" Policy. All such trainings shall occur upon hire, on an annual basis, and periodically as reasonable and appropriate to train workforce members on HIPAA compliance.

HIPAA POLICIES:
GENERAL HIPAA COMPLIANCE AND ENFORCEMENT

Topic: ASSIGNED HIPAA RESPONSIBILITY

Date Adopted: 3/17/2020

I. POLICY

DCG designates an individual with overall responsibility for the DCG HIPAA Compliance Program. The HIPAA Privacy Officer shall be responsible for implementing, overseeing and enforcing all HIPAA requirements applicable to DCG, together with the HIPAA Security Officer, as well as requirements under applicable federal and State law.

II. PROCEDURES

1. Privacy Officer. DCG shall assign overall responsibility for HIPAA compliance, including but not limited to general oversight and management of HIPAA practices, to the HIPAA Privacy Officer. The HIPAA Privacy Officer shall be appointed by Resolution and shall serve for and on behalf of DCG with respect to HIPAA Compliance.
2. Authority of Privacy Officer. The HIPAA Privacy Officer shall have the authority to designate any such HIPAA Compliance responsibilities to appropriate Departments and workforce members as s/he determines is appropriate in order to accomplish designated compliance responsibilities. DCG shall make the identity of the appointed Privacy Officer known to the entire organization so that employees and other workforce members at DCG are aware of whom to contact in the event of a HIPAA or other privacy violation or concern.
3. Defined HIPAA Responsibilities. DCG shall clearly document the Privacy Officer's responsibilities in a written job description reflecting assigned privacy duties and responsibilities of the privacy official, and attached to this Policy as Exhibit "A". Such written job description shall be periodically reviewed by DCG and amended as reasonable and appropriate.

EXHIBIT A

HIPAA Privacy Officer Job Description

- Ensure compliance with HIPAA policies and practices and consistent application of sanctions for failure to comply with the HIPAA Compliance Program for all individuals in the organization's workforce, extended workforce, and for all subcontractors and agents, in cooperation with the HIPAA Committees, as any, the Security Officer, administration, and legal counsel, as applicable.
- Ensure compliance with applicable State and federal laws, and consistent application of regulatory requirements thereunder in accordance with the HIPAA Compliance Program.
- Maintain an accurate inventory of (1) all individuals or third parties who have access to DCG's information, including PHI, (2) all uses and disclosures of such information by any person or entity, including workforce, contractors or agents, and (3) all current HIPAA BAAs, and other contracts and agreements that may affect PHI.
- Manage, monitor and evaluate all aspects of HIPAA Compliance, including appropriate use/disclosure of PHI, respond to and investigate complaints by Individuals or third parties, respond to and manage requests by Individuals for access to, copies of, amendments or restrictions on their PHI, or requests for accountings of disclosures.
- Conduct periodic and routine privacy audits for compliance with the HIPAA Compliance Program and P&S Policies.
- Approve and manage all contracts and agreements, including HIPAA BAAs, that affect or may affect uses and disclosures of PHI by DCG.
- Evaluate and obtain, as necessary, any HIPAA Authorizations prior to use or disclosure of PHI which is not permitted or required by applicable law without authorization.
- Conduct on-going evaluation of the DCG HIPAA Compliance Program together with the Security Officer and HIPAA Committees, if any, to ensure compliance by DCG with applicable HIPAA and related state and federal requirements.
- Initiate, facilitate and promote activities to foster HIPAA privacy awareness within DCG and its various practices.
- Train and communicate to workforce members such applicable HIPAA, state and federal requirements that may be applicable to DCG, including basic HIPAA training, permitted and prohibited uses and disclosures of PHI, minimum necessary uses/disclosures, obtaining HIPAA Authorizations, where necessary, and responding to requests for PHI law enforcement, individuals and other third parties.
- Maintain current knowledge of HIPAA and other applicable federal and state privacy and security laws.
- Work with DCG's administration, legal counsel, and other related parties to represent DCG's HIPAA Privacy interests with external parties (state or local government bodies) who undertake to adopt or amend legislation, regulation, or standard which may affect the DCG HIPAA Program.
- Conduct HIPAA compliance reviews or investigations.
- Serve as HIPAA privacy and compliance resource to DCG and all DCG employees, agents, and other workforce regarding the security and safeguarding of all e-PHI, and all HIPAA privacy and compliance-related issues.
- Such other duties and responsibilities for DCG to fully meet the requirements of HIPAA.

HIPAA POLICIES:
GENERAL HIPAA COMPLIANCE AND ENFORCEMENT

Topic: COMPLAINTS

Date Adopted: 3/17/2020

I. POLICY

DCG will allow individuals, including patients and employees, to report any issue of non-compliance with HIPAA or DCG's P&S Policies. DCG and its employees and other workforces shall not threaten, intimidate or retaliate against any individual filing a complaint pursuant to this Policy. With respect to any such matter, workforce within DCG have direct access to and are encouraged to consult with the Privacy Officer.

II. PROCEDURES

1. Reporting.

   (a) An employee or agent that reasonably believes that: (i) another employee or agent is engaged in conduct which violates or may violate any provision of HIPAA; or (ii) an agent, representative or other person or firm representing DCG in any transaction is engaged in conduct which violates or may violate any provision of HIPAA, shall promptly report such information to the Privacy Officer.

   (b) **Reports** to the Privacy Officer may be made in person, by telephone, in writing or by e-mail to the Privacy Officer.

   (c) The Privacy Officer will maintain written logs regarding HIPAA privacy and security matters, including a record of each complaint filed with or brought to the attention of the Privacy Officer. The person filing or making a complaint or report will not be required to provide his/her name or any other facts that may give away his/her identity. In the event anonymity is requested, the Privacy Officer will use reasonable efforts to keep the identity of the complainant confidential; however, there may be a point in time when the individual's identity may become known or may have to be revealed. The Privacy Officer will encourage the complainant to provide as much information as possible to assist with the investigation of the matter.

   (d) The Privacy Officer will promptly conduct an **investigation** of the report, make a record in the log of the results and the specific actions taken after completion of the investigation, and address any mitigation/disciplinary action which may be required. The specific facts and circumstances surrounding the report should be kept confidential and any discussions regarding the complaints shall be limited to those parties with a "need to know" during the investigation.

   (e) No action should be taken against any employee or agent for the ***good faith reporting*** of any suspected violation of these P&S Policies or other wrongdoing, regardless of whether or not a violation or other wrongdoing is determined to exist following investigation.

2. Documentation. Privacy logs, including the date and nature of each complaint, facts and resolution shall be maintained in a secure location for a period of at least **six (6) years** from the date on which the complaint is filed with the Privacy Officer**.**

HIPAA POLICIES:

ENFORCEMENT

Topic: SANCTIONS

Date Adopted: 3/17/2020

I. POLICY

DCG issues appropriate sanctions against employees or agents who fail to comply with DCG's P&S Policies or the requirements of HIPAA, HITECH and any applicable state laws.

II.PROCEDURES

1. Responsibility for Sanctions. The Privacy Officer will recommend appropriate sanctions for DCG employees or agents who fail to comply with the P&S Policies. DCG's Human Resources department/personnel will apply such appropriate sanctions, as recommended by the Privacy Officer, and consistent with any applicable Human Resources policies and procedures.

2. Application. Sanctions will be administered according to the severity of the failure to comply with these P&S Policies, and the nature of the HIPAA violation. DCG may impose "tiered" levels of sanctions based upon the severity and intent of the HIPAA violation (i.e., intentional vs. unintentional) as it determines to be appropriate. Sanctions may include, but are not limited to:
    - Verbal warning;
    - Written warning;
    - Probation;
    - Suspension;
    - Demotion;
    - Termination from employment;
    - Referral for criminal prosecution (or to other governmental authorities); and/or
    - Demand for reimbursement for any losses or damages resulting from the violation.

3. Documentation. DCG's Human Resources department/personnel, after notifying the Privacy Officer of the imposition of sanctions, will maintain documentation of sanctions that are imposed within each employee's personnel file. Such documentation shall be retained for a period of six (6) years from the effective date of the sanctions.

HIPAA POLICIES: ENFORCEMENT

Topic: TRAINING

Date Adopted: 3/17/2020

I. POLICY

HIPAA privacy and security training shall be provided by DCG to all employees and other workforce members, including management, at least annually, and for all new employees who are beginning employment with DCG. DCG shall ensure that any employees and other workforce who have or may have access to PHI in order to perform their job functions understand and are provided with HIPAA training related to their responsibilities with regard to such information.

II. PROCEDURES

1. The Privacy Officer in consultation with the Security Officer and other appropriate personnel will develop a training strategy by identifying the specific HIPAA Policies that require awareness and training for each type of workforce member, and document them in a *written* "**Privacy** & **Security Awareness and Training Plan"** (attached as Exhibit "A" to this policy). The Privacy Officer will identify specific training strategies and areas of focus, including but not limited to:
    (a) Knowledge of the HIPAA P&S Policies;
    (b) Knowledge of relevant privacy and security laws and regulations, including HIPAA, HITECH, state and other applicable policies and procedures;
    (c) Awareness of DCG's culture of compliance, system-wide monitoring and audit controls;
    (d) Procedures for protecting the confidentiality, availability and integrity of PHI;
    (e) Procedures for authorized uses and disclosures of PHI;
    (f) Procedures to guard against, detect and report any malicious software, security incidents and security breaches, and reporting such to the Security Officer;
    (g) Procedures for safeguarding passwords and usernames;
    (h) Accountability for non-compliance with HIPAA and the P&S Policies; and
    (i) Procedures for reporting any suspected violations of the P&S Policies or HIPAA and related privacy and security laws and regulations to the Privacy Officer.

    As appropriate, the Privacy Officer will assess workforce understanding and effectiveness of the HIPAA Policies through questionnaires, assessments, and other methods in order to determine and address any gaps in workforce members' understanding. Re-training will be provided as appropriate, in connection with other appropriate disciplinary action, including but not limited to where a workforce member violates one or more of the DCG P&S Policies, whether inadvertently or intentionally.
2. The Privacy Officer will be responsible for preparation, updating and implementation of all HIPAA training materials and content, including any written training or refresher materials (i.e., HIPAA "411"

cards, PPTs, Q&As). Trainings will be scheduled and conducted as outlined in the Privacy & Security Awareness and Training Plan or as otherwise determined by the Privacy Officer.

3. The Privacy Officer will work with the Security Officer to disseminate privacy and security messages and updates. Newsletters, screensavers, videotapes, pocket cards, e-mail messages, teleconferencing sessions, staff meetings, and computer-based training and other methods as determined by the Privacy Officer and Security Officer may be used to disseminate information.
4. The Privacy Officer will keep the HIPAA privacy and security awareness and training program fresh and current, and conduct training whenever changes occur in the DCG technology and practices, as appropriate. Annual and periodic training shall be implemented as appropriate department and job responsibilities. The Privacy Officer will incorporate any State laws affecting privacy and security into trainings and updates provided as reasonably necessary.
5. The Privacy Officer will document the date and type of HIPAA training received by workforce, including new hire and periodic training. Documentation will be maintained for a period of six (6) years from the date on which the training was provided.

EXHIBIT B

PRIVACY & SECURITY AWARENESS AND TRAINING PLAN

The Privacy & Security Awareness and Training Plan should outline the following:

- ☐ Training program plan
- ☐ Scope of awareness and training program
- ☐ Goals and objectives
- ☐ Target audiences
- ☐ Deployment methods, evaluation, & measurement techniques
- ☐ Frequency of training

Security Training Category:	GENERAL
Scope of Training:	ENTIRE WORKFORCE (including management)
Training Responsibility:	Privacy Officer
Training Frequency:	Upon Hire, and Annual

1. The Plan: _____
2. Goals: _____
3. Learning objectives:
    - **Privacy & Security Reminders**
    - **State-specific privacy procedures**
    - How to **safeguard PHI**
    - **Permitted and Prohibited uses and disclosures of PHI**
    - How to **protect and guard** the system from **malicious software**
    - How to **monitor log-in attempts** and report discrepancies
    - **Password Management**
    - Incident and Breach reporting to Privacy Officer/Security Officer
    - Accountability/Sanctions
    - Other: _____
4. Deployment methods: _____
5. Evaluation & measurement techniques to be used: _____

Security Training Category:	SPECIFIC:
Scope of Training:	IT
Training Responsibility:	SECURITY OFFICER
Training Frequency:	Upon Hire, and Annual

1. The Plan: _____
2. Goals: _____
3. Learning objectives: _____
4. Deployment methods: _____
5. Evaluation & measurement techniques to be used: _____

Security Training Category:	SPECIFIC:
Scope of Training:	CLINICAL, ADMINISTRATIVE AND SUPPORT STAFF (including management)
Training Responsibility:	PRIVACY OFFICER
Training Frequency:	Upon Hire, and Annual

1. The Plan: _____
2. Goals: _____
3. Learning objectives: _____
4. Deployment methods: _____
5. Evaluation & measurement techniques to be used: _____

HIPAA PRIVACY POLICIES:

INDIVIDUAL RIGHTS

Topic: ACCESS RIGHTS

Date Adopted: 3/17/2020

I. POLICY

1. Each Patient has the right of access to inspect and obtain a copy of his or her PHI in a designated record set, as defined under HIPAA, with the exception of the following:

   (a) "Psychotherapy Notes";

   (b) Information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding;

   (c) Information maintained by DCG that is: (i) subject to the Clinical Laboratory Improvements Amendments of 1988 (CLIA), 42 U.S.C. 262a, to the extent the provision of access would be prohibited by law; or (ii) exempt from CLIA pursuant to 42 C.F.R. 493(a)(2); and

   (d) Information which is reasonably believed by a physician may adversely affect the Patient's mental or physical condition.

To the extent a Patient's PHI is maintained in an ***electronic*** designated record set, such Patient also shall be afforded the right to request a copy of his or her PHI in an electronic form and format of the Patient's choosing, if readily producible, including the provision or transmission of such copy to another individual specifically and clearly designated by the Patient.

II. PROCEDURES

1. Authorization. DCG will request a writing from the Patient specifying the scope of information that the Patient or a third party designated by the Patient wishes to have access to, or copies of. A Patient may be asked for the purpose of the access or copies, but will not be required to provide a response.

2. In-Person Request for PHI. DCG will require all employees, agents and other workforce members to comply with the following with respect to in-person requests for PHI:

   (a) Require the Patient to submit the request for access in writing, specifying the scope of information he/she wishes to have access to or copies of (e.g., all information; billing information; information pertaining to a specific date of treatment).

(b) Require at least one form of identification from the Patient or individual (e.g., driver's license, birth certificate or passport) in order to verify the identity of the individual seeking to obtain access to or a copy of his or her PHI in accordance with Provider's Person or Entity Authentication and Verification for Patients Requesting PHI Policy and Procedures.

(c) Verify that all internal systems, applications or software that may contain the requested PHI are checked. This includes PHI maintained in DCG's medical record system (currently, AthenaHealth) and any other applications or software which comprises DCG's designated record set.

(d) Provide the Patient with the requested PHI as soon as is reasonably possible but in no case later than 30 days. In the event workforce determines that it will take longer than 30 days to produce the requested information, the Privacy Officer will be contacted immediately. [***Note: Although HIPAA permits for a 30 day extension of the response time, the New Jersey Board of Medical Examiner regulations requires Patients to be provided with requested medical record within thirty (30) days.***]

3. Telephone or Fax Requests for PHI. DCG will require workforce to appropriately handle telephone and/or fax requests to release PHI as follows:

(a) Requests for PHI from a Patient made by telephone or fax, provided that the request is made on DCG's Authorization for Release of Records form, may be accepted by DCG in its discretion.

(b) DCG shall make the requested PHI available to the Patient or representative of the Patient via in-person pick-up, by regular postal mail, or through reasonable electronic format, as may be specified in the Authorization. If someone other than the Patient will pick-up the PHI from DCG, the person will be asked to provide proof of identity and authority for pick up.

4. Fees for Copying.

(a) DCG **may charge no greater than one dollar ($1) per page copying fee or $100 for the entire record, whichever is less**. For x-rays and other materials which cannot be routinely copied or duplicated, DCG **may charge no more than the actual cost of the duplication of the materials or the fee charged to DCG for duplication plus an administrative fee of the lesser of ten dollars ($10) or 10 percent of the cost.** DCG may charge an amount not greater than its labor or supplies costs in responding to a Patient's request for a copy of PHI (or a summary or explanation of such information) in an electronic format.

(b) DCG may not charge a fee for copying where:

(1) The request is for a copy of the Patients' medical record where DCG or any of its employed or affiliated physicians has affirmatively terminated the Patient from practice in accordance with the requirements of N.J.A.C. 13:35-6.22; and

(2) An employed or affiliated physician leaves DCG and the Patient requests that his or her medical care continues to be provided by that physician at the physician's new place of practice.

5. Provision of Access. DCG will provide access to or copies of PHI in a timely manner, including arranging with the Patient for a convenient time or location to inspect or copy the PHI, or mailing a copy of the PHI, in the form and format requested by the Patient, if readily producible. Upon the Patient's request, DCG will provide the Patient with electronic copies of any PHI maintained in its **electronic designated record set(s)** in the electronic form and format requested by the Patient, if readily producible in such form and format, or, if not, in a readable electronic form and format as agreed to by DCG and the Patient. If the Patient's request for access directs DCG to transmit the copy of PHI to another individual DIRECTLY, DCG will provide such individual with the copy of the PHI, provided that the Patient submits such a request in writing, which clearly identifies the designated person, where to send the copy of the PHI, and is signed by the Patient.

6. Denial of Patient's Request for PHI.

(a) *Reviewable Grounds for Denial.* DCG may deny requests for access to or copying of PHI, subject to the Patient's right of review, if:

(1) The access requested is likely to endanger the life or physical safety of the Patient or another person or the treating physician in the exercise of professional judgment reasonably believes the Patient would be adversely affected, mentally or physically; (Note: Expressly permitted by NJ BME as grounds for withholding medical records from a patient)

(2) The PHI makes reference to another person, and DCG has determined that the release of the information requested could reasonably lead to harm to that other person;

(3) The request is made by a personal representative of the Patient, and DCG has determined that permitting the access could reasonably cause harm to the Patient.

(b) *Unreviewable Grounds for Denial.* DCG may exclude the following information from the access to or copy of the PHI without providing the Patient with the opportunity to have the denial reviewed: (Note: the following unreviewable grounds for denial are not expressly permitted by the NJ BME as grounds for withholding medical records from a patient. Consult with an attorney before denying access to or copies of such information.)

(1) "Psychotherapy Notes";

(2) Information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding; and

(3) Information maintained by DCG that is: (i) subject to the Clinical Laboratory Improvement Act (CLIA) to the extent the provision of access would be prohibited by law; or (ii) exempt from the CLIA pursuant to 42 C.F.R. 493(a)(2).

(c) If a Patient is denied access to PHI, DCG must:

(1) Notify the Patient why he/she is being denied;

(2) Document the denial in the Patient's file;

(3) Allow the Patient the **right to have the denial reviewed** by a health care professional who is designated by DCG to act as the reviewing official and who did not participate in the original decision to deny the request.; and

(4) Provide, upon request, the copy or a summary of the PHI to the Patient's attorney, health insurance carrier or governmental reimbursement program or agent thereof, with utilization and/or quality of care review responsibility.

7. Business Associate Agreements. Where DCG's Business Associate ("BA") receives a request from a Patient for access to or copies of PHI maintained for or on behalf of a Covered Entity pursuant to a Business Associate Agreement, the terms contained in the BAA as to which entity will bear the burden of production and/or copying of such PHI should be followed. In the absence of any language to the contrary in the applicable Business Associate Agreement, BAs should be instructed to forward any such requests to DCG for DCG to respond to.

8. Disclosures made under this P&S Policy shall be documented and retained for at least six (6) years from the date of the disclosure.

HIPAA PRIVACY POLICIES: INDIVIDUAL'S RIGHTS

Topic: AMENDMENT OF PHI

Date Adopted: 3/17/2020

I. POLICY

DCG will provide each Patient with the right to amend his or her PHI maintained in a Designated Record Set (DRS), as defined by HIPAA, for as long as such PHI is maintained in the DRS by DCG or its Business Associates. DCG may deny a Patient's request for amendment if it determines that the PHI or record that is the subject of the request:

- Was not created by DCG, unless the Patient provides a reasonable basis to believe that the originator of the information is no longer available to act on the requested amendment;
- Is not part of the DRS;
- Would not be available for inspection under HIPAA or applicable law; or
- Is accurate and complete.

II. PROCEDURES

1. Patient's Request for Amendment.

   (a) DCG will permit Patients to submit a request to amend PHI in a DRS maintained by DCG or its Business Associates. All such requests must be made in writing and include a reason to support the requested amendment.
   (b) DCG will act on all requests for amendment as soon as reasonably possible, but **no later than 60 days**** after receipt of the request as follows:

      (1) Immediately upon receipt of a written request, determine whether DCG is obligated under HIPAA or applicable state law to make the requested amendment and, in the event DCG decides it may be necessary to deny the request, provide a written denial to the Patient.

2. Granting Amendment Requests. If DCG grants the requested amendment, in whole or in part:

   (a) DCG will identify the records in the DRS that are affected by the amendment and append the amendment to the original record or otherwise provide a link to the location of the amendment.

(b) DCG will inform the Patient that the amendment is accepted and obtain the Patient's identification and agreement to have DCG notify the relevant persons with which the amendment needs to be shared in accordance with paragraph 2(c) below.

(c) DCG will make reasonable efforts to inform and provide the amendment within a reasonable time to:

(1) Persons identified by the Patient as having received PHI needing the amendment; and

(2) Persons, including Business Associates of DCG, that DCG knows have access to or maintain PHI that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the Patient.

(d) The original information affected by the amendment must remain in the record, with the amendment clearly indicating the information that has been corrected or changed, the date of the change, and the electronic signature of the physician entering the amendment into the record. WORKFORCE SHOULD NEVER CORRECT OR ALTER A RECORD IN A MANNER WHICH WOULD NOT INDICATE THAT AN AMENDMENT HAS BEEN MADE.

3. Denial of Request for Amendment. If DCG determines to deny the requested amendment, in whole or in part:

(a) The denial must be based on DCG's determination that the record or PHI that is the subject of the request:

(1) Was not created by DCG, unless the Patient provides a reasonable basis to believe that the originator of the information is no longer available to act on the requested amendment;

(2) Is not part of the DRS;

(3) Would not be available for inspection under HIPAA or applicable state law; or

(4) Is accurate and complete.

(b) DCG will provide the Patient with a timely, written denial. The denial must use plain language and contain:

(1) The basis for the denial, in accordance with paragraph 3(a) above;

(2) A Patient's right to submit a written statement disagreeing with the denial and how the Patient may file such a statement;

(3) A statement that, if the Patient does not submit a statement of disagreement, the Patient may request that DCG provide the Patient's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment; and

(4) A description of how the Patient may complain to DCG pursuant to the complaint procedures established by DCG. DCG will include the name, title, and telephone number of the Privacy Officer.

4. Statement of Disagreement. DCG will permit the Patient to submit a written statement disagreeing with any denial of all or part of a requested amendment and the basis of such disagreement. All written statements of disagreement shall be forwarded to the Privacy Officer immediately upon receipt.

5. Rebuttal Statement. The Privacy Officer or his or her designated representative shall prepare a written rebuttal to the Patient's statement of disagreement, and provide the same to the Patient.

6. Recordkeeping. DCG will identify the record or PHI in the DRS that is the subject of the disputed amendment and append or otherwise link the Patient's request for an amendment, DCG's denial of the request, the Patient's statement of disagreement, if any, and Provider's rebuttal, if any, to the DRS.

7. Future Disclosures.

   (a) If a statement of disagreement has been submitted by a Patient, DCG will require the Inclusion of the material appended in accordance with paragraph 2.(e) above, or, at the election of Provider, an accurate summary of any such information, with any subsequent disclosure of the PHI to which the disagreement relates. If the Patient has not submitted a written statement of disagreement, DCG must include the Patient's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the PHI only if the Patient has requested such action in accordance with paragraph 2.(b)(iii) above.

   (b) When any subsequent disclosure is made using a standard transaction that does not permit the additional material to be included with the disclosure, DCG may separately transmit the material required by these procedures to the recipient of the standard transaction.

8. **If DCG is unable to act on the request for amendment within **60 days,** DCG, with the approval of the Privacy Officer, may extend the time for such action by no more than 30 days provided that DCG provides the Patient, within the initial 60 day time period, with a written statement of the reasons for the delay and the date DCG will complete its action on the request. DCG may have only one such extension of time for action on a request for an amendment.

9. Implementation Specification. Upon receipt of notice by DCG from another Covered Entity of an amendment to a Patient's PHI, DCG will append the amendment to the original record or otherwise provide a link to the location of the amendment.

10. Patient requests for amendment as well as the titles of the persons and/or offices responsible for receiving and processing requests for amendments must be documented and retained in a secure location for **six (6) years** from the date of the request for amendment.

HIPAA PRIVACY POLICIES:
INDIVIDUAL'S RIGHTS

Topic: ACCOUNTING OF DISCLOSURES

Date Adopted: 3/17/2020

I. POLICY

DCG affords each Patient the right to request and receive an accounting of certain disclosures of PHI made by DCG or its Business Associates. DCG will maintain all information that may be required to respond to an individual's request for an accounting under HIPAA for a period of **six (6) years** from the date on which the accounting is requested. All requests for accountings must be submitted by the individual in writing to DCG.

II. PROCEDURES

1. Accountings. Upon written request, DCG will provide a Patient with an accounting of all disclosures of PHI made by DCG, its employees, agents and other workforce members, as well as DCG's Business Associate's, within a period of **six (6) years** from the date of the request, except the following disclosures which are excluded from such "accounting" requirement:

    (a) Those made to carry out treatment, payment or healthcare operations;

    (b) Those made to the Patient him/herself;

    (c) Those that are merely incidental to another permissible use or disclosure;

    (d) Those made as a result of a listing in the facility directory;

    (e) Those made to friends and family members, provided that the Patient agreed to the disclosure and did not object to the disclosure, or which were made based on professional judgment that the disclosure was necessary;

    (f) Those made pursuant to a HIPAA valid Authorization;

    (g) Those made for national security or intelligence purposes;

    (h) Those made to corrections institutions or law enforcement officials having custody of inmates;

    (i) Disclosures made as part of a limited data set; and

(j) Disclosures made using de-identified information.

2. Business Associates. DCG will require Business Associates to provide such information as would be needed in order for DCG to respond to an individual's request for an Accounting as required by § 164.528. Business Associates should not respond directly to any requests for an accounting and should direct all requests for accountings directly to DCG.

3. Written Requirements for Provision of Accounting

(a) *Written Accounting.* The written accounting provided shall include:

(1) The date of each disclosure,

(2) The name of each entity or person who received the PHI, and if known, the address of such entity or person;

(3) A brief description of the type of PHI disclosed; and

(4) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, a copy of the individual's authorization, or a copy of a written request for a disclosure.

(5) For multiple or "routine" disclosures (those where DCG has made multiple disclosures of PHI to the same person or entity for a single purpose or pursuant to a single authorization), the accounting may provide:

a. The information required above for the first disclosure during the accounting period;
b. The frequency, periodicity or number of disclosures made during the accounting period; and
c. The date of such last disclosure during the accounting period.

4. Form and Format. DCG will provide an accounting in a form and format requested by the individual if readily producible in that format; if not readily producible in that format, then provision in hard copy or other form and format that may be reasonable to the individual and Provider. Reasonable and appropriate safeguards must be in place to deliver an accounting to the individual.

5. Accounting Logs. Any workforce who make a "non-excepted" disclosure shall make a notation in the Accounting Log (see attached Exhibit A) (or through an equivalent documentation mechanism) of the date, name of person who received the PHI, a brief description of the PHI disclosed and a brief statement of the purpose of the disclosure. Disclosures to the following persons/entities at a minimum must be documented by DCG and made available for an accounting (*note that this is not an exclusive list*):

(a) **Release of PHI to an "authorized individual"** (i.e., any governmental authority authorized by law to receive reports of abuse, neglect or domestic violence such as protective or social services agencies, state survey and certification agencies, ombudsmen for the aging

for those in long-term care facilities, law enforcement or oversight) **about Victims of Abuse, Neglect or Domestic Violence.**

(b) **Release of PHI for Public Health Activities to Public Health Authorities** authorized by law to collect or receive information in order to prevent or control disease, injury or disability, including reporting disease, injury, vital events such as birth or death and conducting public health surveillance, investigations and interventions and to report cases of child abuse or neglect, including the Food and Drug Administration, the Occupational Safety and Health Administration, the Centers for Disease Control and Prevention and state and local public health departments.

(c) **Release of PHI for Health Oversight Activities** (e.g., oversight of health care plans, oversight of health benefits plans, oversight of health care providers, oversight of health care and health care delivery, oversight of activities that involve resolution of consumer complaints, oversight of pharmaceuticals, medical products and devices, and a health oversight agency's analysis of trends in health care costs, quality, health care delivery, access to care, health insurance coverage for health oversight purposes, audits, civil, administrative or criminal investigations, inspection, licensure or disciplinary actions and civil, administrative or criminal proceedings and actions) to Health Oversight Agencies (e.g., an agency or authority of the U.S., a State, a territory or political subdivision of a State or territory or an Indian Tribe that is authorized by law to oversee the health care system or government programs in which health information is necessary to determine eligibility or compliance or to enforce civil rights laws for which health information is relevant. Examples of these are: State insurance commissions, State health professional licensure agencies, Offices of Inspector Generals, the Department of Justice, State Medicaid fraud control units, the Health and Human Services Office for Civil Rights, the Office of the Attorney General and the FDA.)

(d) **Release of PHI to Avert a Serious Threat to Health or Safety to a Person or the Public.**
(e) **Release of PHI to a Person/Entity Responsible for Payment of Worker's Compensation Benefits to the Patient.**
(f) **Release of PHI for Military and Veterans Activities;**
(g) **Release of PHI for Government Programs providing Public Benefits;**
(h) **Release of PHI to Funeral Directors/Homes**
(i) **Release of PHI to the Medical Examiner or Coroner**
(j) **Release of PHI to Law Enforcement**
(k) **Release of PHI to Organ Donation Activities**

6. Timeframe for Response. DCG must act on the Patient's request for an accounting **no later than 60 days** after receipt of the request. In the event DCG is unable to provide an accounting within 60 days, DCG may extend the time to provide the accounting by no more than 30 days, provided that DCG advises the Patient with a written statement of the reasons for the delay and date by which it will provide the accounting. DCG may only have one such extension.

7. Cost and Fees. DCG must provide one accounting per year without charge. Thereafter, DCG may impose a reasonable, cost-based fee for each subsequent request within the same 12-month period, provided that the Patient is informed in advance of the cost.

8. The Privacy Officer shall be notified of each request for an accounting and will direct the provision of such reports and review each response prior to its provision to the Patient. A copy of the

accounting must be maintained in the Patient's file for a period of six (6) years from the date on which the applicable report was produced.

9. DCG will temporarily suspend a Patient's right to receive an accounting of disclosures to a health oversight agency or law enforcement official for the time specified by such agency or official if the agency/official provides DCG with a written statement that: 1) such an accounting to the individual would be reasonably likely to impede the agency's activities; and 2) specifying the time for which the suspension is required. If the agency or official statement is made orally: (1) document the statement, including the identity of the agency or official making the statement; (2) temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and (3) limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

HIPAA PRIVACY POLICIES:

INDIVIDUAL'S RIGHTS

Topic: REQUEST FOR RESTRICTIONS & CONFIDENTIAL COMMUNICATIONS

Date Adopted: 3/17/2020

I. POLICY

1. Requests for Restrictions. DCG permits Patients to request that DCG, or its Business Associates, restrict: (i) Uses or disclosures of PHI to carry out treatment, payment, or health care operations; and (ii) disclosures for which DCG must provide an individual with the opportunity to agree or to object under 42 C.F.R. § 164.510. DCG MUST comply with an individual's request to restrict certain disclosures which are made to health plans for payment or health care operations purposes where DCG has been paid in full and out of pocket by the individual (or the individual's authorized representative) for the specific services.

2. Confidential Communications. DCG permits Patients to request, and will accommodate ***reasonable requests*** by Patients, to receive communications of PHI from DCG by alternative means or at alternative locations.

II. PROCEDURES

1. Right of a Patient to Request Restriction of Uses and Disclosures.

   (a) DCG will afford every Patient the right to request that DCG or its Business Associates restrict the following uses and disclosures of PHI. Except as provided in Section II.1.(a)(iii) below, DCG is not required to grant a Patient's request where the restriction relates to:

      i. Uses or disclosures of the Patient's PHI to carry out treatment, payment, or health care operations; and

      ii. Disclosures for which DCG must provide the Patient with the opportunity to agree or to object under 42 C.F.R. § 164.510 (e.g. disclosures to assist in the notification of family members).

      iii. Disclosures, except as otherwise provided by law, which pertain to a disclosure to a health plan for purposes of carrying out payment or health care operations, and not for purposes of carrying out treatment, and the PHI pertains SOLELY to a health care item or service for which DCG has been paid out of pocket in full. DCG must comply with a request from and individual to restrict these disclosures.

   (b) DCG will include in its HIPAA Notice of Privacy Practices a statement that Patients have the right to request restrictions on uses and disclosures of their PHI, and that with the exception of as set forth in Section II.1.(a)(iii), that DCG is not required to agree to the restriction.

(c) DCG will require requests for restrictions to be submitted in writing. The requestor's authority to request such restriction shall be evaluated as may be necessary (e.g., in cases of legal representatives).

(d) All requests for restrictions shall be forwarded to the Privacy Officer for review. If the Privacy Officer grants the restriction, the restriction shall be honored by implementing the restriction in the Patient's files at DCG through such mechanisms for restricting use/disclosure in DCG's electronic medical record or other application (i.e.,"sequester" the files, or mark or otherwise **flag** them as "restricted").

(e) Any Business Associate(s) which may be affected by a restriction agreed upon by DCG should promptly be provided notice of such. DCG will require all Business Associates to agree in their respective Business Associate Agreements that they will abide by any restrictions on disclosures of PHI of which DCG makes them aware of.

(f) Where a restriction is in place, DCG will not use or disclose PHI in violation of such restriction, except that, if the Patient who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment, DCG may disclose the restricted PHI to a health care provider to provide emergency treatment to the Patient. A restriction agreed to by DCG is not effective to prevent uses or disclosures permitted or required under C.F.R. §§ 164.502(a)(2)(ii), 164.510(a) or 164.512.

(g) Notwithstanding a restriction agreed upon by DCG as required in accordance with Section II.1.(a)(iii), the agreed upon restriction may only be terminated if:

i. The Patient agrees to or requests the termination in writing;

ii. The Patient orally agrees to the termination and the oral agreement is documented; or

iii. DCG informs the Patient that it is terminating its agreement to a restriction, except that such termination is only effective with respect to PHI created or received *after* it has so informed the individual; or

iv. Otherwise required by law.

2. <u>Right of a Patient to Request Confidential Communications.</u>

(a) DCG will permit a Patient the right to request that confidential communications be received by alternative means or at alternative locations.

(b) All requests for confidential communications shall be made in writing.

(c) DCG will accommodate reasonable requests.

(d) DCG may condition the provision of a reasonable accommodation on:

i. When appropriate, information as to how payment, if any, will be handled; and

ii. Specification of an alternative address or other method of contact.

3. Documentation related to a Patient's request for restrictions or confidential communications shall be maintained in a secure location by the Privacy Officer for a period of **six (6) years** from the date of the request**.**

HIPAA PRIVACY POLICIES:
INDIVIDUAL'S RIGHTS

Topic: PERSONAL REPRESENTATIVES WITH LEGAL AUTHORITY

Date Adopted: 3/17/2020

I. POLICY

DCG allows personal representatives who have *legal authority* (hereinafter, a "Personal Representative") to act on behalf of a Patient as if such Personal Representative were to have "stepped into the shoes" of the Patient for purposes of access to and use of the Patient's PHI relevant to such personal representation.

II. PROCEDURES

1. Prior to releasing PHI to a person claiming to be a Personal Representative, DCG will require verification of the person's authority as follows:

   (a) Request identification from the person to determine whether such person has authority to act as a personal representative on behalf of a Patient in making decisions related to health care (e.g., spouse, other next of kin, Court Order appointing Guardian; Power of Attorney etc.).

   (b) If the documentation or representation is sufficient to demonstrate that the requesting individual is an authorized Personal Representative of the Patient, treat such person as a Personal Representative, with respect to PHI relevant to the personal representation. **Ensure that the minimum necessary PHI is only released to such representative in accordance with the scope of their authority (e.g., limited guardian, special medical guardian).**

   (c) If the documentation is not sufficient to ensure that the requesting individual is an authorized Personal Representative of the Patient, the PHI may not be released to the requesting individual unless a written Authorization from the individual has been obtained, or the disclosure may be permitted under Provider's Family Member, Relatives and Friends Policy and Procedure.

   (d) DCG may not treat any parent, guardian or other person as a Personal Representative of an **unemancipated minor** if the minor has the authority to make decisions with respect to PHI pertaining to a health care service under State law, such as for pregnancy, sexually transmitted disease, or substance use. *See* DCG's Policy and Procedures governing Minors. This includes but is not limited to HIV/AIDS positive test results and related information for minors age 12 and up.

   (e) DCG shall **NOT** treat a person as the Personal Representative of the Patient if there is reasonable belief that:

(1) the Patient has been or may be subjected to violence, abuse or neglect by such person; or

(2) treating such person as the Personal Representative could endanger the Patient and in the exercise of professional judgment, it is not in the best interest of the Patient to treat the person as the Patient's Personal Representative.

(f) For release of **HIV/AIDS records**, see DCG's "HIV/AIDS Information" Policy for a list of those specific individuals authorized by N.J.S.A. 26:5C-12 to receive such information.

(g) Contact and notify the Privacy Officer in the event a negative determination is made regarding the release of PHI or if the authority of the requesting individual to act as the Personal Representative is questionable.

HIPAA PRIVACY POLICIES:

USE AND DISCLOSURE OF PHI

Topic: TREATMENT

Date Adopted: 3/17/2020

I. POLICY

DCG uses or discloses PHI for purposes of treating patients with which it has an established relationship. DCG does not required prior written or verbal authorization to be obtained prior to any disclosure of PHI for treatment purposes unless otherwise required by applicable State law.

II. PROCEDURES

1. Definitions.

   (a) *"Treatment"* is defined as "the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another."

   (b) All other terms have the meanings ascribed to them by HIPAA, HITECH and other applicable state and federal law.

2. A signed Authorization need not be obtained prior to the use or disclosure of *pertinent* PHI between licensed physicians and other practitioners where the physician or other licensed practitioner, in the exercise of professional judgment, determines it would be in the best interests of the Patient and the disclosure of PHI would be to another licensed health care professional who is providing or has been asked to provide treatment to the Patient, or whose expertise may assist the physician or other licensed practitioner in his or her rendition of professional services.

3. Disclosures for treatment purposes through a health information exchange organization (HIO) may only be in accordance with other federal and state laws and guidelines governing such disclosures. At all times, DCG will require that its employees, agents and other workforce members comply with the policies and procedures of any HIO in which it participates and exchanges patient PHI. DCG will consult with legal counsel to the extent necessary with respect to any uses or disclosures of PHI made through such HIO including but not limited to disclosures of sensitive information for treatment purposes.

HIPAA PRIVACY POLICIES:
USE AND DISCLOSURE OF PHI

Topic: FAMILY MEMBERS, RELATIVES or FRIENDS

Date Adopted: 3/17/2020

I. POLICY

PHI may be disclosed to a family member, other relative, or a close personal friend of a Patient, or any other person identified by a Patient, so long as: (i) the information is *directly relevant* to the requesting individual's *involvement* with the Patient's health care or payment related to the Patient's healthcare; *and* (ii) the Patient has agreed to the disclosure, been provided with the opportunity to object to the disclosure and the Patient does not so object, or it can be reasonably inferred from the circumstances, based on professional judgment, that the Patient does not object.

If the Patient is not present or otherwise unable to object, DCG will use its best professional judgment to determine whether the disclosure of the Patient's PHI to a family member, other relative, or close personal friend would be in the Patient's best interest. Only the minimum amount of PHI shall be disclosed to such individual as necessary.

II. PROCEDURES

1. DCG employees, agents and other workforce members ("Personnel") shall:

    (a) Presume that the Patient would not want the family member, relative or friend to have access to the PHI, unless there is information clearly indicating the contrary.

    (b) Clarify whether a Patient desires to share PHI with any family members, relatives or friends by routinely attempting to obtain written or other permission listing those individuals with whom DCG may share PHI.

    (c) Determine and document any family members, relatives or friends or other individuals to whom the Patient does not want his or her PHI disclosed to, and if so, document such patient preferences.

2. Unless otherwise indicated by the Patient and documented as set forth in II.1 above, DCG should ***not disclose*** PHI to a family member, relative or personal friend (or other person(s) identified by the Patient) except under the circumstances set forth below:

    (a) Notification of Family Members. DCG may use or disclose PHI to notify, or assist in the notification of (including identifying or locating), a family member, relative, or another person responsible for the care of the Patient of the Patient's location, general condition, or death.

(b) If the Patient is Present. If the Patient is present or available, and has the capacity to make health decisions, DCG may disclose PHI to a family member, relative or other person identified by the Patient, so long as DCG:

(1) Obtains the Patient's agreement; or

(2) Provides the Patient with the opportunity to object to the disclosure, and the Patient does not object; or

(3) Reasonably infers from the circumstances, based on the exercise of professional judgment, that the Patient would not object to the disclosure.

(c) If the Patient is Not Present or the Patient is Incapacitated or in an Emergency Circumstance.

(1) If the Patient is not present or available, or the opportunity to agree or object to the disclosure is not practicable because the Patient is incapacitated or in an emergency circumstance, DCG may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the Patient and, if so, disclose only the PHI that is directly relevant to the person's involvement with the Patient's health care or payment related to such Patient's health care or needed for notification purposes.

(2) DCG may allow a person to act on behalf of the Patient to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of Patient information, even without an Authorization or the Patient's express agreement if, in the professional judgment of DCG's administrator or agent, it is in the Patient's best interest to allow the practice.

3. DCG may make limited use or disclosure of PHI for disaster relief purposes to public or private entities, authorized by law or charter to assist in disaster relief efforts, for the purpose of coordinating with such entities any use or disclosures permitted for notification purposes as set forth in §164.510(b)(1)(ii), subject to the same requirements set forth above in Section II.2.(b) and (c), and provided that DCG, in the exercise of professional judgment, determines that such requirements do not interfere with the ability to respond to the emergency circumstances.

4. DCG may elect NOT to disclose PHI to a family member, relative or friend of the Patient, if DCG has reasonable belief that:

(a) The Patient has been or may be subjected to domestic violence, abuse or neglect by such person; or

(b) Disclosing PHI could endanger the Patient; and DCG, in the exercise of professional judgment, decides that it is not in the best interest of the Patient to disclose PHI.

HIPAA PRIVACY POLICIES:
USE AND DISCLOSURE OF PHI

Topic: EMERGENCY SITUATIONS

Date Adopted: 3/17/2020

I. POLICY

DCG may use or disclose PHI where it reasonably believes the use or disclosure may be necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or to the public or necessary for law enforcement authorities to identify or apprehend an individual as a result of such individual's statement admitting participation in a violent crime that may have caused serious physical harm to the victim or where apparent that the individual escaped from a correctional institution or other lawful custody.

II. PROCEDURES

1. DCG may use or disclosure PHI as permitted under this P&S Policy **without** the individual's authorization or giving the individual an opportunity to agree or object.

2. DCG shall at all times comply with the "Minimum Necessary" Standard P&S Policy and under HIPAA and HITECH, as may be modified from time to time.

3. Aversion of serious and imminent threats. Consistent with applicable law and standards of ethical conduct, pertinent **PHI may be disclosed** to a law enforcement agency or other health care professional when there is a belief, in good faith, and in the exercise of professional judgment, that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of the Patient or another person; and Provider is reasonably able to prevent or lessen the threat, including the target of the threat. N**otwithstanding this section, DCG shall not release any HIV/AIDS related information unless would otherwise be specifically permitted by law and DCG's HIV/AIDS Information P&S Policy.**

4. **[Note that the New Jersey Board of Medical Examiners permits more limited disclosures to law enforcement as described in Section 3 above for aversion of *serious and imminent harm* or as required by law, although HIPAA would be far more permissible. Therefore, as DCG is subject to the BME regulations, it is restricted to disclosures pursuant to Section 3, unless it would otherwise be required by law to disclose PHI to law enforcement, such as for reporting of gunshot wounds.]** Law Enforcement. Consistent with applicable law and standards of ethical conduct and the above Section 3 of this Policy and Procedures, **PHI may be disclosed** to law enforcement authorities for the purposes described above to avert serious and imminent threat to the health or safety of the individual, another person, or the public, if required by law to make such disclosure.

a. Because of a written or oral statement by an individual admitting participation in a violent crime that DCG reasonably believes may have caused serious physical harm to the victim; HOWEVER:

(1) *Use or disclosure not permitted*. DCG may NOT use or disclose PHI when the information is learned by DCG:

1. In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure, or counseling or therapy; or

2. Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy.

(2) *Limit on information that may be disclosed*. A use or disclosure under these circumstances shall contain only the following:

a. The statement made by the individual admitting participation in the violent crime; and

b. The following PHI:

(i) Name and address,
(ii) Date and place of birth,
(iii) Social security number,
(iv) ABO blood type and rh factor,
(v) Type of injury,
(vi) Date and time of treatment,
(vii) Date and time of death (if applicable), and
(viii) Description of distinguishing characteristics (such as height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos).

OR

(b) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.

5. Disclosures made under this Policy shall be made pursuant to DCG's Accounting of Disclosures P&S Policy, and retained for a period of six (6) years from the date of the disclosure.

HIPAA PRIVACY POLICIES:
USE AND DISCLOSURE OF PHI

Topic: DECEASED PATIENTS

Date Adopted: 3/17/2020

I. POLICY

If under applicable law, an executor, administrator, or other person has authority to act on behalf of a deceased individual (the "Decedent") or of the individual's estate, DCG will treat such person as a legal Personal Representative of the individual. To the extent permitted by State law, DCG may also release the PHI of a decedent to any family member or other person identified and permitted under the circumstances set forth in DCG's Family Members, Friends and Relatives P&S Policy, unless doing so would be inconsistent with any prior expressed preference of the Patient.

Disclosures to any other third party (e.g., coroner; funeral director etc) of a Decedent's PHI shall permitted only if handled in accordance with the following procedures. Where disclosure of information is sought and it has been **fifty (50) years** since the date of decedent's death, such information shall no longer considered PHI and may be disclosed without any authorization from a legal Personal Representative. Notwithstanding the foregoing, to the extent such information would still be protected by State and other applicable laws and regulations, DCG will continue to extend such protections to the Decedent's information to the extent required by law.

II. PROCEDURES

1. Prior to releasing the Decedent's PHI, DCG will verify the requesting individual's authority to determine whether the person has the authority, as an executor, administrator, trustee, or other authorized person, to act on behalf of the Decedent or the Decedent's estate, or to request information about the Decedent,

2. If the requesting individual provides documentation sufficient to ensure that he/she is authorized to receive information regarding the Decedent, DCG will treat such person as a Personal Representative with respect to the PHI relevant to the Personal Representative.

3. To the extent permitted by State law, in the event the individual requesting Decedent PHI would be considered a family member, relative or other individual involved in the Patient's care or payment of such care prior to his or her death as set forth in DCG's Family Members, Relatives or Friends P&S Policy, DCG may release such PHI to the individual as relevant to his or her involvement in the Decedent's care or payment of such care, even if such person would not have the legal authority to act on behalf of the Decedent, or the Decedent's estate. Notwithstanding the foregoing, if DCG knows of a prior expressed preference of the Decedent that such Patient would not have wanted such individual to have access to the PHI, DCG will not release or provide PHI to such family member or other person.

4. The Decedent's PHI may be disclosed to a **coroner** or **medical examiner** for the purpose of: (i) identifying a deceased person, (ii) determining a cause of death, or (iii) other duties as authorized by law. DCG will obtain verification of requesting individual's authority.

5. The Decedent's PHI may be disclosed to **funeral directors**, consistent with applicable law, as necessary to carry out their duties with respect to the Decedent. If necessary for funeral directors to carry out their duties, PHI may be disclosed prior to, and in reasonable anticipation of, the individual's death.

6. The Decedent's PHI may be disclosed to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

7. Disclosures made under this P&S Policy will be made pursuant to DCGs Accounting of Disclosures P&S Policy and retained a period of six (6) years from the date of the disclosure.

8. Where an individual has been deceased for fifty (50) years or more, DCG may treat such individual's information as information which is not PHI and therefore not subject to these policies and procedures, except to the extent such information would still be protected by State and other applicable laws and regulations.

HIPAA PRIVACY POLICIES:
USE AND DISCLOSURE OF PHI

Topic: PAYMENT

Date Adopted: 3/17/2020

I. POLICY

DCG may use and disclose PHI for purposes of receiving payment for health care services provided to its Patients. Except as otherwise may be required by applicable State or federal law, DCG does not require prior written or verbal authorization prior to disclosing PHI for appropriate payment related purposes.

II. PROCEDURES

1. Definitions.

   (a) *"Payment"* includes the activities undertaken by: (1) a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or (2) a covered health care provider or health plan to obtain or provide reimbursement for the provision of health care.

   (b) All terms not otherwise defined have the meanings ascribed to them by HIPAA, HITECH and other applicable state and federal law.

2. The activities referenced in the definition of Payment relate to the individual and include, but are not limited to:

   (a) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

   (b) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

   (c) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

   (d) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

(e) Utilization review activities, including pre-certification and preauthorization of services, concurrent and retrospective review of services; and

(f) Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement: Name and address, date of birth, social security number, payment history, account number and name and address of the health care provider and/or health plan.

3. Signed Authorization Not Needed. Except as otherwise required by applicable State or federal law, a signed Authorization need not be obtained from the individual prior to the use or disclosure of PHI if such use or disclosure is:

   (a) For the purposes of carrying out DCG's *own* payment operations;

   (b) To another Covered Entity (e.g., health care provider, payer or clearinghouse) for Payment activities of the receiving Covered Entity;

4. DCG will require any vendor or contractor conducting payment activities on DCG's behalf to enter into a HIPAA Business Associate Agreement to the extent such vendor or contractor would have access to, or which would create, receive, maintain or transmit PHI in connection with the performance of payment activities on DCG's behalf (i.e., debt collection company, third party billing and coding company).

5. An individual shall have the right to request a restriction on a disclosure for payment purposes to a health plan IF it relates solely to a health care item or service for which the individual has paid for in full and out-of-pocket as set forth in DCG's Request for Restrictions and Confidential Communications P&S Policy.

HIPAA PRIVACY POLICIES:
USE AND DISCLOSURE OF PHI

Topic: HEALTHCARE OPERATIONS

Date Adopted: 3/17/2020

I. POLICY

DCG's employees, agents and other workforce members may use Patient PHI in order to conduct DCG's own health care operations activities. Except as otherwise required by applicable State or federal law, prior written or verbal authorization is not required from the Patient prior to using or disclosing PHI for DCG's health care operations purposes.

II. PROCEDURES

1. Definitions.

(a) *"Health Care Operations"* is defined to include any of the following activities of DCG or of another Covered Entity to the extent that the activities are related to covered functions, and any of the following activities of an organized health care arrangement in which DCG or such Covered Entity participates:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities, patient safety activities (as defined in 42 CFR 3.20), population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and Patients with information about treatment alternatives; and related functions that do not include treatment;

(2) Conducting quality assessment and improvement;

(3) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

(4) Most underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance);

(5) Conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection and compliance programs;

(6) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(7) Business management and general administrative activities of the Covered Entity, including, but not limited to:

(i) Management activities relating to implementation of and compliance with the requirements of this subchapter;
(ii) Customer services, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.
(iii) Resolution of internal grievances;
(iv) Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a covered entity or, following completion of the sale or transfer, will become a covered entity; and

(b) All terms not otherwise defined have the meanings ascribed to them by HIPAA, HITECH and other applicable state and federal law.

2. Signed Authorization Not Needed. Except as otherwise required by applicable State or federal law, a signed Authorization need not be obtained prior to the use or disclosure of PHI if such use or disclosure is:

a. For the purposes of carrying out DCG's *own* Health Care Operations functions;

b. To another Covered Entity for such Covered Entity's own Health Care Operations, *as long as* (i) the entity either has (or had) a relationship with the Patient, (ii) the information pertains to such relationship and (iii) the disclosure is either:

i. For the purposes of conducting quality assessment and improvement activities or reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing or credentialing activities; or
ii. For the purpose of health care fraud and abuse detection or compliance.

c. To another Covered Entity that participates with DCG in an Organized Health Care Arrangement for any health care operations activities of the Organized Health Arrangement.

3. An individual shall have the right to request a restriction on a disclosure for health care operations purposes to a health plan IF it relates solely to a health care item or service for which the individual has paid for in full and out-of-pocket as set forth in DCG's Request for Restrictions and Confidential Communications P&S Policy.

HIPAA PRIVACY POLICIES:
USE AND DISCLOSURE OF PHI

Topic: BUSINESS ASSOCIATES

Date Adopted: 3/17/2020

I. POLICY

DCG requires that all independent contractors and vendors who may have access to, or which may create, maintain, receive or transmit, PHI for or on behalf of DCG enter into a Business Associate Agreement with DCG to appropriately safeguard PHI and prohibit impermissible uses and disclosures of PHI.

II. PROCEDURES

1. Definitions.

(a) A "Business Associate" means a person who, with respect to a Covered Entity:

(1) On behalf of such Covered Entity or of an organized health care arrangement (as defined in this section) in which the Covered Entity participates, but other than in the capacity of a member of the workforce of such Covered Entity or arrangement, creates, receives, maintains, or transmits protected health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing or

(2) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such Covered Entity, or to or for an organized health care arrangement in which the Covered Entity participates, where the provision of the service involves the disclosure of protected health information from such Covered Entity or arrangement, or from another business associate of such Covered Entity or arrangement, to the person.

(3) ***A "business associate" includes a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.***

(b) A "Subcontractor" means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

2. Access to PHI by Business Associates. DCG will require only those independent contractors and vendors who have a legitimate and appropriate need to use and disclose PHI in order to perform a service or function for or on behalf of DCG have access to such PHI. Access to or use of PHI by such

independent contractors and vendors must be limited to the minimum necessary to perform their responsibilities for or on behalf of DCG in accordance with DCG's Minimum Necessary P&S Policy.

3. Business Associate Agreement.

(a) DCG will require that each independent contractor and/or vendor seeking to access or use PHI enters into a HIPAA compliant Business Associate Agreement (BAA) *prior to permitting access to such PHI*. DCG may utilize the Checklist for Reviewing Third Party HIPAA Business Associate Agreements before entering into any BAA with a Business Associate using the Business Associate's own form of BAA.

(b) A HIPAA compliant BAA shall include at a minimum the following provisions:

(1) Establishment of the permitted and required uses and disclosures of PHI that the Business Associate may make for or on behalf of DCG;

(2) That the Business Associate will:

a. Not use or further disclose PHI other than as permitted by the BAA or as required or permitted by law, in any manner which would violate HIPAA If done by the covered entity, and comply with all applicable requirements of the Privacy and Security Rules;
b. Use appropriate safeguards to prevent unauthorized use or disclosure of PHI and implement reasonable and appropriate administrative, technical and physical safeguards to protect the confidentiality, integrity and availability of electronic PHI;
c. Ensure any agent to whom Business Associate provides PHI agrees to implement reasonable and appropriate security measures to protect the information;
d. Report to DCG any use or disclosure of PHI which is not provided for by the BAA, including but not limited to a Breach of PHI;
e. Ensure that any subcontractors that will receive any of DCG's PHI agree to the same restrictions and conditions that apply to it with respect to the PHI and enter into a HIPAA compliant BAA with the Business Associate;
f. Make PHI available in accordance with an individual's Access Rights;
g. Make PHI available for Amendment and Incorporate any Amendments granted by DCG;
h. Make information available as required for DCG and/or Business Associate to provide an Accounting of Disclosures;
i. To the extent Business Associate is to carry out DCG's obligations under the Privacy or Security Rule, comply with the requirements of the Privacy or Security Rule that would apply to DCG in the performance of such obligation; and
j. Make its internal books, practices and records relating to the use or disclosure of DCG's PHI available for inspection by the Secretary of HHS for purposes of determining DCG's compliance with HIPAA.

(3) That Business Associate must report any Security Incidents or Breaches to DCG as

soon as reasonably practicable but in any case no later than **sixty (60) days** from the actual or constructive discovery of the Security Incident or Breach by Business Associate.

(4) That DCG may terminate the BAA in the event that the Business Associate materially breaches or violates the BAA, and such breach cannot be reasonably cured;

(5) That upon termination of the BAA, all PHI must be returned or destroyed by the Business Associate and/or subcontractors, including any copies, or if not feasible, extend the protections of the BAA to the information and limit all further use and disclosure to those purposes that make the return or destruction of the information infeasible.

4. Monitoring of Business Associates.

(a) DCG will actively monitor all Business Associates for compliance with the respective BAAs. In the event DCG becomes aware that a Business Associate has engaged in a pattern of activity or practice that would violate the terms of the BAA, DCG must notify Business Associate of such material breach and, in the event Business Associate fails to cure such Breach, terminate the BAA.

(b) DCG will require that all appropriate employees, agents and other workforce members are appropriately trained in the uses and disclosures of PHI which Business Associates may have access to, including but not limited to ensuring that only the minimum necessary amount of PHI is provided to Business Associates as needed to perform their obligations under the terms and conditions of the BAA.

5. Documentation. All BAAs will be retained for a period of **six (6) years** from the date of their expiration or termination.

HIPAA PRIVACY POLICIES:
USE AND DISCLOSURE OF PHI

Topic: PROHIBITION ON "SALE" OF PHI

Date Adopted: 3/17/2020

I. POLICY

DCG does not, and does not permit its Business Associates to, sell PHI. DCG will not directly or indirectly accept any remuneration *in exchange* for a Patient's PHI without first obtaining a valid HIPAA-Authorization which includes a specific statement that remuneration will be received in connection with the use and disclosure of the Patient's PHI.

DCG (or its Business Associate) may, without having to first obtain a valid HIPAA-Authorization, directly or indirectly receive remuneration in connection with uses and disclosures of PHI for any of the permitted purposes (for purposes of this Policy, individually, each a "Permitted Purpose" and collectively, the "Permitted Purposes") as set forth by this P&S Policy.

II. PROCEDURES

1. No "Sale" of PHI. DCG shall not accept remuneration, financial or otherwise, direct or indirect, in exchange for disclosing PHI except as otherwise permitted by this Policy or pursuant to a HIPAA Authorization from the individual who is the subject of the PHI. A "sale" of PHI will be deemed to have occurred if DCG is primarily being compensated by or on behalf of the recipient of data to supply the data it maintains in its role as a covered entity or business associate.

2. No Authorization Required. The individual's prior written authorization is not required for any of the Permitted Purposes set forth below in Section 2. The Privacy Officer shall be responsible for determining whether a use and/or disclosure is a Permitted Purpose where DCG or its Business Associate is to receive any money, either directly or indirectly, in connection with a specific use or disclosure of a Patient's PHI. However, the Patient's Consent shall still be obtained where required to comply with State law unless otherwise specifically indicated where the disclosure would be to a Business Associate or other third party or entity.

3. Permitted Purposes. The following are Permitted Purposes for which remuneration may be received by DCG or its Business Associates without authorization from the individual, unless otherwise required by State law, as follows:

(a) The purpose of the exchange is for Public Health Activities (45 CFR § 164.512(b) or 45 CFR § 164.514(e));

(b) The purpose of the exchange is for Research pursuant to 45 CFR §164.512(i) or § 164.514(e), and the only remuneration received by DCG is a reasonable cost-based fee to cover the costs of preparation and transmittal of the data for such purpose;

(c) The purpose of the exchange is for the Treatment of the individual pursuant to 45 CFR §164.506(a), or for Payment, subject to any regulation that the Secretary may promulgate to prevent PHI from inappropriate access, use, or disclosure;

(d) The purpose of the exchange is a Health Care Operation concerning the Sale, Transfer, Merger, or Consolidation of all or part of DCG with another Covered Entity, or an entity that following such activity will become a Covered Entity, and due diligence related to such activity pursuant to paragraph (6)(iv) of the definition of health care operations and 45 CFR §164.506(a);

(e) The purpose of the exchange is for remuneration that is provided to or by DCG to a Business Associate for activities involving the exchange of PHI that the Business Associate undertakes on behalf of and at the specific request of DCG pursuant to a Business Associate Agreement and §§164.502(e) and 164.504.(e);

(f) The purpose of the exchange is to provide an individual with Access and a copy of the Patient's PHI or accounting of disclosures (45 CFR §§ 164.524 or 164.528);

(g) The purpose of the exchange is Required by Law (45 CFR § 164.512(a)); or

(h) The purpose of the exchange is otherwise permitted by and in accordance with the Privacy Rule where the only remuneration received by the Covered Entity or Business Associate is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or otherwise permitted expressly by other law.

4. Authorization Required. If the use or disclosure is not any one of the Permitted Purposes, then DCG will require the Patient's written authorization for receipt of remuneration.

5. If a third party has presented a signed "HIPAA-compliant" Authorization from the individual, the Privacy Officer shall review and confirm the validity of that document, which must include the following elements in accordance with HIPAA & the HITECH Act:

(a) All of the elements set forth on DCG's Checklist for Valid Authorizations;

AND

(b) *A statement that the use or disclosure of the requested information will result in direct or indirect remuneration to DCG from a third party*.

5. DCG will provide a copy of the signed Authorization to the Patient. DCG will maintain a copy of the signed Authorization, or an electronic copy, for a period of 6 years from the date of its creation, or the date when it was last in effect, whichever is later.

HIPAA PRIVACY POLICIES:

USE AND DISCLOSURE OF PHI

Topic: DE-IDENTIFIED INFORMATION

Date Adopted: 3/17/2020

I. POLICY

Information that has been rendered "**de-identified**" under HIPAA and in accordance with this Policy, with respect to which there is no reasonable basis to believe that the information can be used to identify an individual, directly or indirectly, may be treated by DCG as no longer being covered by HIPAA and the P&S Policies. DCG may use PHI to create information that is de-identified or disclose PHI to a business associate for such purpose, whether or not the de-identified information is ultimately to be used by DCG.

II. PROCEDURES

1. Any health information that meets the standard and implementation specifications for de-identification under 45 CFR § 164.514(a) and (b) is considered not to be individually identifiable health information can be treated as "de-identified" and not PHI protected by HIPAA and the DCG P&S Policies. Information that has been de-identified in accordance with the applicable requirements of § 164.514 and this Policy may be treated as such, provided that:

    (a) Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of PHI; and

    (b) If de-identified information is re-identified, DCG may use or disclose such re-identified information only as permitted or required by the HIPAA Privacy Rule and the DCG P&S Policies.

    DCG may de-identify PHI as reasonable and appropriate for the operation of its practice as set forth in Sections 2 and/or 3 of this Policy, as required by §164.514(b).

2. In order for PHI to be **"de-identified"** for purposes of the Expert Determination Method (§ 164.514(b)(1)), DCG must engage a person with "appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable", who, applying such principles and methods:

(a) determines that the *risk is very small* that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

(b) Documents the methods and results of the analysis that justify such determination.

3. In order for PHI to be "**de-identified"** for purposes of the Safe Harbor Method (§ 164.514(b)(2)), ALL OF THE FOLLOWING IDENTIFIERS related to the individual, the individual's employers, and the individual's household members MUST BE REMOVED:

(a) Names;

(b) All geographical subdivisions smaller than a state (thus, indications of street address, city, precinct, zip code, and their equivalent geocodes must be removed, *except for* the first three initial digits of the ZIP code, if, according to the current publically available data from the Bureau of the Census (i) the geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people and (ii) the initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000);

(c) All elements of dates (except years) related to an individual, such as dates of birth, admission, discharge, or death. All ages of 90 and above must be removed (and in such cases, the year must be removed); provided, however, that such ages may be described as a single category of "age 90 or older" (i.e., reported as "on or before 1920);

(d) Telephone numbers;

(e) Fax numbers;

(f) Electronic mail addresses; Web Universal Resource Locators ("URLs"); and Internet Protocol ("IP") addresses;

(g) Social security numbers;

(h) Medical record numbers (including prescription numbers);

(i) Health plan beneficiary numbers;

(j) Account numbers;

(k) Certificate and license numbers;

(l) Vehicle identifiers, including serial and license plate numbers;

(m) Device identifiers and serial numbers;

(n) Web Universal Resource Locators;

(o) Internet Protocol (IP) addresses;

(p) Biometric identifiers, including finger and voice prints;

(q) Full face photographic images and any comparable images; and

(r) Any other unique identifying number, code, or characteristic. An illustrative but non-exhaustive list of unique identifiers include:

- Unusual occupations (i.e., current occupation as President at State A University);
- Very high salary ranges;
- Existence/location of unique birthmarks and scars; and
- That fact that a health condition or injury was the result of an unusual or highly publicized source or event, where there is a reasonable belief that disclosure of such fact would permit identification of the individual (such as, for example, an individual's receipt of anthrax-laden letters or mail bombs or falling victim to acts of terrorism or sniper attacks).

4. DCG MUST ENSURE that, *to its knowledge*, after the above-described identifiers have been removed, the information may not be used alone or in combination with other information to identify an individual who is a subject of the information.

(a) PHI may not be treated as De-Identified where DCG or its Business Associate(s) on its behalf would have "*actual knowledge"* that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

(b) "Actual knowledge" does not include mere knowledge of the existence of specific studies about methods to re-identify or use de-identified health information alone or in combination with other information to identify an individual.

(c) Actual knowledge does include clear and direct knowledge that the remaining information could be used, either alone or in combination with other information, to identify an individual who is the subject of the information, i.e., concluding that the remaining information could be used to identify the individual.

5. DCG may consider, as applicable, additional guidance issued by the Secretary of HHS, regarding de-identification pursuant to the Safe Harbor and Expert Determination methods, available at **http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html**

HIPAA PRIVACY POLICIES:
USE AND DISCLOSURE OF PHI

Topic: MARKETING

Date Adopted: 3/17/2020

I. POLICY

DCG will obtain a signed written HIPAA Authorization from a Patient before it uses or disclosures any PHI for communications defined by HIPAA as "Marketing" EXCEPT unless otherwise permitted by this Policy. Treatment and health care operations, where remuneration is received, will also be considered marketing activities requiring a HIPAA Authorization for purposes of this Policy.

II. PROCEDURES

1. Definitions.

   (a) "Marketing" is any communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

   (b) "Financial remuneration" is any direct or indirect payment from or on behalf of a third party whose product or service is being described, excluding payment for the treatment of a Patient. A direct payment is one that flows from a third party whose product or service is being described DIRECTLY to DCG. An Indirect payment is one that flows from an entity on behalf of a third party whose product or service is being described to Provider.

2. Authorization Needed. All employees, agents and other workforce members, as well as Business Associates of DCG, are required to obtain prior written HIPAA Authorization from a Patient before using or disclosing any PHI for communications which would be considered "marketing." The Privacy Officer must be consulted before any PHI is used or disclosed for communications which could potentially be considered "marketing.

   (a) Communications where DCG would receive financial remuneration will be considered marketing and require a HIPAA Authorization prior to the use or disclosure of PHI for such purposes. **This includes treatment and health care operations purposes conducted *in exchange* for remuneration where the communication encourages purchase or use of a product or service offered by the third party, including but not limited to:**

      (1) **Appointment reminders**

      (2) **Treatment reminders**

      (3) **Alternative treatments**

      (4) **Health care products or services**

(b) Communications which would be considered marketing do not require a HIPAA Authorization where they are in the form of:

(1) A face-to-face communication ***made by*** DCG to the Patient; or

(2) A promotional gift of nominal value ***provided by*** DCG.

3. DCG will treat any statement that ***encourages recipients of the communication to purchase products or to use services*** as "Marketing" and obtain a HIPAA Authorization **UNLESS** such communication is made:

(a) For treatment of the Patient, including case management or care coordination for the Patient, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the Patient, **PROVIDED THAT** DCG does NOT receive financial remuneration in exchange for making the communication; or

(b) To provide refill reminders or other communications concerning drugs or biologics currently being prescribed to the Patient, but *only if* any financial remuneration received is *reasonably related* to DCG's cost of making the communication (i.e., supplies, labor and postage);

(c) For the following health care operations activities, *except where financial remuneration is received in exchange for making the communication*:

(1) To describe a health-related product or service (or payment for such product or service) that is provided by or included in a plan of benefits of DCG making the communication, including communications about: (i) the entities participating in a health care provider network or health plan network or health plan network; (ii) replacement of, or enhancements to, a health plan; and (iii) health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.

(2) For case management or care coordination, containing of individuals with information about treatment alternatives and related functions to the extent such activities do not fall within the definition of treatment.

4. In addition, DCG may be required to treat arrangements between DCG and any other entity whereby DCG discloses PHI to the other entity, or receives PHI from the other entity, in exchange for financial remuneration in order to **allow the *other* entity, or DCG on behalf of the other entity,** to communicate **about its *own* product** or **service**, as "Marketing".

5. The following are generally NOT required to be treated as "Marketing", *except where financial remuneration is received in exchange for making the communication:*

(a) Mailings promoting health in a general manner; *for example*:

(1) Reminding females to get an annual physical;

(2) Providing information about how to control diabetes;

(3) Information about new developments in health care (e.g., new diagnostic tools);

(4) About health or "wellness" classes;

(5) About support groups;

(6) About health fairs.

(b) Communications about government and government-sponsored programs such as Medicaid, supplemental benefits, or SCHIP;

(c) Calendars, pens, and the like that display the name of a product or entity (but only when provided by DCG).

6. When considering whether a communication is "Marketing," the Privacy Officer should consider whether the effect of the communication meets the definitional criteria of "Marketing." *It is irrelevant whether or not the intent of the communication was for marketing purposes*. All questions concerning clarification as to whether a communication is "Marketing" shall be directed to the Privacy Officer.

7. If it is determined that a communication is "Marketing," DCG shall require a signed HIPAA Authorization from the Patient prior to using or disclosing PHI for Marketing purposes. The Authorization shall specify what PHI is being disclosed and for what purpose, *and that financial remuneration will be received in exchange for making the communication.*

8. DCG shall **NOT** seek or obtain a **"Blanket Authorization"** for Marketing which are **expressly PROHIBITED** under HIPAA. DCG shall obtain a signed HIPAA Authorization from the Patient each time DCG wishes to patient PHI for a purpose other than described on a previous signed Authorization.

9. Disclosures made under this Policy shall be made pursuant to DCG's Accounting of Disclosures P&S Policy, and documentation retained for at least six (6) years.

HIPAA PRIVACY POLICIES:

USE AND DISCLOSURE OF PHI

Topic: FUNDRAISING

Date Adopted: 3/17/2020

I. POLICY

DCG may use or disclose certain demographic information or dates of health care provided to a patient without obtaining that patient's signed written authorization for fundraising purposes. DCG may use or disclose to a Business Associate or to DCG's institutionally-related foundation, if any, (the "Foundation") **Demographic Information** (defined below) of, or **dates** of health care provided to, a patient for purposes of raising funds for its own benefit, only as permitted by this Policy.

If DCG desires to use and disclose additional PHI for fundraising purposes other than as described above, DCG will obtain a signed Authorization Form for CE to Use and Disclose PHI from the Patient and otherwise use and disclose such information *only in compliance with* all other P&S Policies governing the use and disclosure of PHI.

II. PROCEDURES

1. To the extent fundraising activities may or will be conducted, DCG may use or disclose only the following limited PHI to a Business Associate or applicable Foundation for fundraising purposes without obtaining prior written Authorization from the Patient:

    a. Demographic Information;

    b. Dates of health care provided to the Patient;

    c. Department of service information;

    d. Treating physician;

    e. Outcome information; and

    f. Health insurance status.

2. The term "Demographic Information" shall be limited to: a Patient's name, address and other contact information, age, gender, and dates of birth. Demographic Information does NOT include any information about a Patient's diagnosis or treatment. Accordingly, disease or "condition-specific" letters targeted to Patients requesting contributions are expressly prohibited. Any such mailings must be directed to the general population.

3. DCG may compile a list containing the information permitted by Section 1 of this Policy (hereafter the "Fundraising List"). The Fundraising List must only be used by DCG or provided to a Business Associate or Foundation for purposes of contacting the Patients on the list regarding fundraising for DCG.

4. When providing the Fundraising List to a Business Associate or Foundation, DCG must obtain assurances that such information will only be used in accordance with this Policy. A copy of this section should be provided to the Business Associate or Foundation.

5. DCG must provide Business Associate or Foundation with the name and contact information of the individual at DCG who is responsible for maintaining an updated Fundraising List.

6. DCG, its Business Associate or Foundation, may use the Fundraising List in order to, from time to time, contact the Patients listed therein for purposes of soliciting funds for the benefit of Provider.

7. Permissible fundraising activities may include, but are not limited to, appeals for money and sponsorship of events. Royalties or remittances for the sale of products of third parties are generally NOT considered permissible fundraising activities, except in instances where royalties or remittances come from auctions, rummage sales, and similar activities.

8. PDCG, its Business Associate or Foundation may determine the best means of contacting Patients on the Fundraising List.

9. If DCG, its Business Associate or Foundation sends fundraising materials to Patients on the Fundraising List, such materials must provide a *clear and conspicuous* description of how the Patient may "opt-out" of receiving any further fundraising communications.

    (a) The method to "opt-out" may not cause the Patient an undue burden or more than a nominal cost, such as a toll-free number, an email address or similar mechanism. A written letter of opt-out is specifically considered to be an "undue burden."

    (b) Each such fundraising communication sent to a Patient must include information on how the individual may opt-out. DCG may choose whether to implement an opt-out mechanism *globally* (i.e., opt-out of all future fundraising communications of any type) or *specific to a given fundraiser*.

10. If a Patient exercises his or her right to NOT receive any further fundraising communication, DCG or its Business Associate or the Foundation must immediately and permanently remove that individual's information from its Fundraising List. DCG must ensure that once an individual exercises his or her right to NOT receive further fundraising communications, he or she will not receive them in the future.

11. If there are multiple holders of the Fundraising list, the entity that receives notification that a Patient wishes to have his or her information removed from the Fundraising List must immediately contact the staff-member at DCG responsible for updating the Fundraising List and inform him or her that such Patient wishes to be removed from the Fundraising List.

12. The staff-member at DCG must remove that Patient's information from the Fundraising List. The staff-member must then provide an updated Fundraising List to all holders of such list. The Fundraising List must bear the date of the most recent update.

13. DCG shall, to the extent that it conducts fundraising activities as set forth in this Policy, amend its Notice of Privacy Practices to ensure that it includes a statement that DCG may or does engage in fundraising activities, and that a Patient may opt out of receiving such communications. The Notice need not describe specifically *how* a Patient may opt out of receiving fundraising communications; rather, such information must be included on each fundraising communication sent to the Patient.

14. Documentation regarding an individual's exercise of the right to opt-out of fundraising communications shall be retained for a period of at least six (6) years by the designated fundraising department.

HIPAA PRIVACY POLICIES:
USE AND DISCLOSURE OF PHI

Topic: PUBLIC HEALTH ACTIVITIES

Date Adopted: 3/17/2020

I. POLICY

DCG may disclose PHI to certain public health or government authorities or to certain individuals, under the circumstances and public health activities and purposes described in this P&S Policies.

II. PROCEDURES

1. Written Authorization Not Needed. DCG may disclose PHI to the following authorities or persons, for the public health activities and purposes described below without obtaining written authorization from the individual:

    a. To a **public health authority or foreign government agency official** that is authorized by law to collect or receive the PHI being disclosed, such as the New Jersey State Department of Health, *for the purpose of* preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions;

    b. At the direction of a public health authority, to an **official of a foreign government agency** that is acting in collaboration with a public health authority;

    c. To a public health authority or other **appropriate government authority** authorized by law to receive reports of *child abuse or neglect*;

    d. To a **person subject to the jurisdiction of the Food and Drug Administration** (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, *for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity*. Such purposes include:

        (1) To collect or report adverse events (or similar reports with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;

        (2) To track FDA-regulated products;

        (3) To enable product recalls, repairs, or replacement or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or

(4) To conduct post-marketing surveillance.

e. To a **person** who may have been **exposed to a communicable disease** or may otherwise be **at risk of contracting or spreading a disease or condition**, *as Provider is authorized by law to notify such person in the conduct of a public health intervention or investigation*.

f. For immunization purposes, except as otherwise prohibited by State law, to a **school** about an individual who is a **student or prospective student** of the school, if:

(1) The PHI that is disclosed is limited to *proof of immunization*;

(2) The school is required by State or other law to have such proof of immunization prior to admitting the individual; and

(3) DCG obtains and documents (i.e., notation in medical record) the *agreement to the disclosure* from either:

a. The parent, guardian or other person acting in loco parentis of the individual, if the individual is an unemancipated minor; or
b. The individual, if the individual is an adult or emancipated minor.

2. Disclosure under this Policy may be made without first obtaining a signed Authorization or giving the individual an opportunity to agree or object.

3. Except for disclosures that are made pursuant to an Authorization (even though one is not required for disclosures under this Policy) or where required by law, disclosures under this Policy must comply with DCG's "Minimum Necessary" P&S Policy.

4. Disclosures made under this Policy shall be made pursuant to DCG's Accounting of Disclosures P&S Policy, and retained for six (6) years. For public health disclosures that reoccur on a regular basis, documentation may be satisfied by a statement reflecting the "regular reporting schedule" to a particular public health care agency. As much of the following information should be obtained regarding the disclosure as possible:

a. **Date and time** of the disclosure, and whether the disclosure was made orally or in writing (a copy of any writing should be kept in the record);

b. **Description** of the PHI disclosed;

c. **Name, title, and government affiliation** of the person(s):

i. Representing that disclosure is necessary;

ii. Requesting disclosure; and

iii. Receiving the PHI disclosed;

d. The **factual basis** for the belief that disclosure is necessary, including:

(1) Representations made by a person or entity that caused DCG to believe that disclosure was necessary;

(2) DCG's basis for believing that the person making the representations had knowledge about the situation; and

(3) DCG's basis for believing that the person making the request and/or receiving the PHI had the authority to request and/or receive it.

HIPAA PRIVACY POLICIES:

USE AND DISCLOSURE OF PHI

Topic: HEALTH OVERSIGHT ACTIVITIES

Date Adopted: 3/17/2020

I. POLICY

DCG may disclosure PHI to a health oversight agencies for oversight activities authorized by law, including: (1) audits; (2) civil, administrative or criminal investigations; (3) inspections; (4) licensure; (5) disciplinary actions; (6) civil, administrative or criminal proceedings or actions; (7) other activities necessary for appropriate oversight of:

(1) The health care system;

(2) Government benefit programs for which health information is relevant to beneficiary eligibility;

(3) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or

(4) Entities subject to civil rights laws for which health information is necessary for determining compliance.

If a health oversight activity or investigation is conducted *in conjunction with* an oversight activity or investigation relating to a claim for *public benefits* not related to health, DCG *may* disclose PHI to a health oversight agency in such instance.

II. PROCEDURES

1. Employees will direct unique requests for release or access to PHI from a health oversight agency to the attention of the Privacy Officer.

2. Confirmation that the request is made by a "health oversight agency" must be made prior to releasing PHI. A "health oversight agency" includes an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Native American tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is "authorized by law" to oversee the health care system (whether private or public) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

3. Once it is confirmed that the request is made by a "health oversight agency," the PHI may be released without having to obtain an authorization and without providing the individual with an opportunity to agree or object to the disclosure.

4. When a request centers around **the Patient who is the subject of an investigation by a health oversight agency**, PHI (about that Patient) may be disclosed to the requesting health oversight agency **ONLY IF** such investigation or other activity "*arises out of*" and is "*directly related to*" either:

   (a) The receipt of health care;

   (b) A claim for public benefits related to health; or

   (c) Qualification for, or receipt of, public benefits or services, when the individual's health is integral to the claim for public benefits or services.

5. Where the **Patient is the subject of an investigation** and such investigation or activity *does not* "arise out of" and is not "directly related to" the preceding activities described in (1)-(3) above, DCG may **NOT** disclose PHI under this procedure. In such case, the procedure governing disclosures of PHI for Law Enforcement Purposes should be followed.

6. Disclosures made under this Policy shall be made pursuant to DCG's Accounting of Disclosures P&S Policy and documentation retained for six (6) years.

HIPAA PRIVACY POLICIES:
USE AND DISCLOSURE OF PHI

Topic: REQUIRED BY LAW

Date Adopted: 3/17/2020

I. POLICY

DCG may use and disclose PHI only to the extent required by law. Additional requirements shall be met prior to the release of PHI if such disclosure relates to: Victims of Abuse, Neglect or Domestic Violence; or for Law Enforcement purposes. For disclosures relating to these excepted topics, DCG shall meet the requirements described in the corresponding Policies and Procedures, Victims of Abuse, Neglect or Domestic Violence or Law Enforcement Purposes.

II. PROCEDURES

1. Routine Uses and Disclosures. DCG is responsible for identifying current federal and state laws that mandate certain *routine* disclosures of PHI. The Privacy Officer, or his/her designee, will maintain a list of state and federal laws (statutes and regulations) that require DCG to make ***routine*** uses and disclosures of certain PHI. DCG employees may consult this list to determine if a disclosure is one that DCG is routinely legally mandated to make, and, if it is, the PHI may be disclosed as required by law. For example, DCG's physicians must report gunshot wounds, suspected or actual incidents of child abuse or neglect, or elder abuse or neglect, or when an individuals' treatment is the subject of peer review.

2. Disclosures to BME or Attorney General. DCG will disclose PHI pursuant to a demand for a statement in writing or a subpoena issued by the Board of Medical Examiners or the Office of the Attorney General, to the extent its physicians would be required to do so by law.

3. Requests to Disclose PHI. Requests for release of PHI that an individual or entity claims is "required by law" will be directed to the Privacy Officer. The Privacy Officer must first determine whether the disclosure is **mandated** (versus merely permitted). If the use or disclosure is mandated, the Privacy Officer must disclose PHI in accordance with this Policy. If the use or disclosure is merely permitted, the Privacy Officer is not permitted to make the use or disclosure under this Policy and Procedures. In such case, the Privacy Officer should determine if the use or disclosure is permitted under another Policy. If the use or disclosure is not permitted under any other Policy, DCG may **NOT** disclose the PHI without first obtaining an Authorization for CE to Use and Disclose PHI.

4. ***Required by law*** means a ***mandate of law***, enforceable in a court of law, that would compel DCG to make a use or disclosure of PHI. Examples of mandates that would be deemed "required by law" include:

   (a) Statutes or regulations that require use or disclosure of PHI;

   (b) Court orders and court-ordered warrants;

   (c) Subpoenas or summons issued by a court, grand jury or administrative body.

5. Once the Privacy Officer confirms that the request is required by law, the Privacy Officer, or employee as directed by the Privacy Officer, may disclose the PHI without having to obtain an Authorization and without providing the Patient with an opportunity to agree or object to the disclosure, provided that the disclosure is made in accordance with this policy and the Privacy Officer, or employee:

   (a) Verifies the authority of the requestor;

   (b) Verifies the identity of the requestor in accordance with the procedure governing Person or Entity Authentication and Verification for Patients Requesting PHI; and

   (c) Documents the disclosure in accordance with the P&S Policy governing Accounting for Disclosures and maintains this documentation in the patient's record for six (6) years.

Topic: RESPONDING TO SUBPOENAS *

Date Adopted: 3/17/2020

I. POLICY

DCG will not disclose PHI pursuant to a subpoena or other discovery request unless permitted under HIPAA and applicable state law. (Note: New Jersey may prohibit disclosure pursuant to a subpoena or discovery request which is NOT accompanied by a court order, *even if* HIPAA's "satisfactory assurances are obtained. Consult with an attorney in the event a subpoena or discovery request is received *prior to disclosure of PHI thereunder.*)

II. PROCEDURES

1. **ANY AND ALL SUBPOENAS AND DISCOVERY REQUESTS SHOULD BE IMMEDIATELY DIRECTED TO THE PRIVACY OFFICER AND LEGAL COUNSEL.**

2. **DCG complies with HIPAA "satisfactory assurances" prior to disclosing PHI pursuant to a subpoena or discovery request. In the event that "satisfactory assurances" are not provided, the subpoena/discovery request must be returned and the requestor can be informed that the HIPAA requirements have not been met.** DCG will comply with any more stringent New Jersey requirements which may require a court order to accompany the subpoena/discovery request even if "satisfactory assurances" are obtained.

3. Disclosure of PHI. PHI may be disclosed in the following circumstances only:

   (a) In Accordance with a **signed Authorization**.

   (b) In Accordance with an **Order of a Court** or Other "Administrative Tribunal." (see Law Enforcement Requests P&S Policy)

   (c) In Accordance with a **Civil Subpoena/Discovery Request** under the Following Circumstances:

      (1) The subpoena or discovery request contain **one of the two** following items:

         a. Proof that reasonable efforts have been made to provide written notice to the individual that his or her PHI Is being sought; OR

         b. Proof that the Attorney has applied to the court for a "**qualified protective order**". In order to satisfy this requirement, must show that:

(i) the parties in the lawsuit have agreed to a "qualified protected order" and have presented their agreement to the court; or

(ii) that a "qualified protective order" has been requested from the court that would limit the use of PHI. The term "qualified protective order" means an order of a court or a stipulation by the parties to the litigation that:

- Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which the information was requested; and

- Requires the return of the PHI (including all copies) to the originating source at the end of the litigation.

4. This Policy does <u>not</u> apply to:
   (a) Court orders
   (b) Court issued subpoenas (including grand jury subpoenas)
   (c) Search warrants; and/or
   (d) Summonses issued by a court.

5. Disclosures made under this Policy shall be made pursuant to DCG's <u>Accounting of Disclosures</u> P&S Policy, and retained for six (6) years.

Responding to a subpoena can have significant legal and other consequences. Consult with an attorney as soon as reasonably possible after obtaining a subpoena, warrant or other summons that would or potentially might result in disclosure of PHI.* *<u>Do not</u>*** *rely solely on this Policy to respond in any such circumstance. <u>This Policy does not constitute legal advice with regard to subpoena and other requests for PHI.</u>*

HIPAA PRIVACY POLICIES:
USE AND DISCLOSURE OF PHI

Topic: LAW ENFORCEMENT REQUESTS

Date Adopted: 3/17/2020

I. POLICY

DCG may release PHI to law enforcement officials and for law enforcement purposes if such disclosure is "required by law," is enforceable in a court of law, and is released only in strict accordance with this Policy. DCG will consult with Legal Counsel to determine whether any of these disclosures of PHI would require Patient Consent for purposes of State law.

This Policy DOES **NOT** APPLY to investigations that arise out of and are directly related to: (1) the receipt of health care, (2) a claim for public benefits related to health **OR** (3) qualification for, or receipt of public benefits or services where an individual's health is integral to the claim for benefits or services. In such cases, the P&S Policy governing Health Oversight Activities should be followed. Furthermore, if the individual is not the SUBJECT of the investigation, the P&S Policy governing Health Oversight Activities *may* be applied.

II. PROCEDURES

1. **ANY AND ALL REQUESTS FOR PHI MADE BY A LAW ENFORCEMENT OFFICER MUST BE IMMEDIATELY DIRECTED TO THE PRIVACY OFFICER AND LEGAL COUNSEL.**

2. PHI may be disclosed in compliance with the relevant requirements of:

   (a) A Court Order or Court-Ordered Warrants;

   (b) A Subpoena or Summons issued by a judicial officer;

   (c) A Grand Jury Subpoena; or

   (d) An Administrative Request, including an administrative subpoena or summons, a civil or an authorized investigative demand or similar process authorized under law, such as the New Jersey Board of Medical Examiners or the New Jersey Attorney General's Office, provided that:

      (1) The information sought is relevant and material to a legitimate law enforcement inquiry;

      (2) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

      (3) De-identified Information could not reasonably be used.

3. DCG will limit any disclosures made pursuant to this Policy to only the minimum amount necessary to comply with the request made pursuant to a requirement of law.

4. Suspects, Fugitives, Material Witnesses, or Missing Persons. **ONLY** the following PHI may be disclosed in response to a law enforcement official's request for suspects, fugitives, material witnesses, or missing persons**:**
   (a) Name and Address;
   (b) Date and Place of Birth;
   (c) Social Security Number;
   (d) ABO blood type and rh factor;
   (e) Type of Injury;
   (f) Date and Time of Treatment;
   (g) A description of distinguishing physical characteristics, including, height weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos;
   (h) Date and time of death (if applicable).

5. The foregoing limited PHI ***may*** be provided at the oral or written request of someone acting on behalf of law enforcement (e.g., in response to a radio or television broadcast for assistance in identifying a suspect, "Wanted" posters and other public service announcements). PHI related to the individual's **DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue** are **NOT to be disclosed** for the purpose described in the above paragraph. See DCG's Genetic Information Policy and Procedures for release of genetic information. PHI related to the individual's **HIV/AIDS status or related information** are likewise **NOT to be disclosed** for the purpose described in the above paragraph. See DCG's HIV/AIDS Information P&S Policy for release of HIV/AIDS related information.

6. For requests by law enforcement in connection with ***Victims of Crime***, the Patient must be given an opportunity to agree or disagree before any PHI about the Patient is released for such purpose. Thus, except as required by law, DCG may **NOT** disclose PHI pursuant to a law enforcement official's request for such information about a Patient who is, or is suspected to be, a victim of a crime unless it has been determined that the individual consents to such a disclosure.

7. If an individual's consent cannot be obtained because of incapacity or other emergency circumstances, the PHI **may still be disclosed provided that:**

   (a) The law enforcement official represents that such information is ***needed*** to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;
   (b) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be ***materially and adversely affected*** by waiting until the individual is able to agree to the disclosure; AND
   (c) The disclosure is in the ***best interests*** of the individual as determined by Provider, in the exercise of professional judgment.

8. This Policy does not prevent reporting under state mandatory reporting laws regarding certain crime victims. Disclosure of PHI concerning victims of abuse, neglect or domestic violence must be in compliance with the P&S Policy Victims of Abuse, Neglect or Violence. This Policy also does not prevent reporting under State mandatory reporting laws regarding gunshot wounds or communicable diseases.

9. This Policy is not intended to restrict the ability of a physician, in the exercise of his or her professional judgment, who has a good faith belief that a patient because of mental or physical condition may pose an imminent danger to him/herself or others, from releasing *pertinent information* to a law enforcement agency or other health care professional in order to minimize the threat of danger in accordance with N.J.A.C. 13L35-6.5(d), subject to HIPAA as set forth in this Policy at Section 6, with the exception of HIV/AIDS information, which may only be released in strict compliance with N.J.S.A. 26:5C-8 and DCG's Policy governing HIV/AIDS Information.

10. With regard to requests by law enforcement in connection with a ***Decedent***, PHI may be disclosed to a law enforcement official in order to alert such officials that the death of the individual may have resulted from criminal conduct.

11. With regard to requests by law enforcement in connection with a "***Crime on Premises",*** PHI may be disclosed to a law enforcement official if DCG believes, in good faith, it constitutes evidence of criminal conduct that occurred on the premises of DCG and disclosure would prevent or lessen the threat to the health or safety of the individual or another person.

12. Disclosures made under this Policy shall be made pursuant to DCG's Accounting of Disclosures P&S Policy, and retained for six (6) years.

HIPAA PRIVACY POLICIES:

USE AND DISCLOSURE OF PHI

Topic: VICTIMS OF ABUSE, NEGLECT OR VIOLENCE

Date Adopted: 3/17/2020

I. POLICY

DCG may disclose, in accordance with this Policy, PHI about an individual that DCG reasonably believes is a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, that is authorized by law to receive such reports. This policy excludes reports of child abuse or neglect that are mandated by law,

II. PROCEDURES

1. Except for mandated reports of child abuse or neglect (which are covered by the " Public Health Activities" and "Required by Law" policies) an employee, agent or other workforce member of Provider who, in his/her professional judgment, reasonably believes that an individual has been a victim of abuse, neglect, or domestic violence (*e.g., victim of spousal abuse or abuse*) can disclose PHI about the victim to a government authority that is authorized by law to receive reports of such abuse, neglect, or domestic violence (*e.g., adult protective services)* in the following circumstances:

a) **Required by law:** If the disclosure is required by law, disclosure is permitted only if it is limited to the extent of such law's requirements. "Required by law" means that there is some mandate of the law, enforceable in court, that compels DCG to make the disclosure. *Example: If a disclosure about a victim of abuse, neglect or domestic violence is made in response to a court order, permitted disclosures are limited to that PHI required to be disclosed by the face of the court order.*

b) **Consent:** Disclosure is permitted if the victim authorizes to the disclosure. The agreement can be written or verbal; if verbal, the victim's consent will be documented.

c) **Authorized by law:** Disclosure is permitted to the extent the disclosure is expressly authorized by statute or regulation and:

(1) DCG, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the victim or other potential victims; or

(2) If the victim cannot agree because he or she is incapacitated, when a law enforcement or other public official authorized to receive the report represents to a DCG employee that:

i. The victim's PHI will not be used against the victim, and

ii. An immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the victim is no longer incapacitated.

2. Informing the individual.

a) The victim must be promptly notified, in writing or orally, that such a report has been or will be made, *except if, in the exercise of professional judgment*:

(1) DCG believes that informing the victim would place him or her at risk of serious harm *(e.g., potential physical or emotional harm from learning that a report was made)*; or

(2) DCG would be informing a Personal Representative, and DCG reasonably believes the Personal Representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interest of the victim as determined by DCG.

b) DCG will document notification of the victim as follows:
(1) If the victim is informed orally, a notation should be made in the record;
(2) If the victim is informed in writing, a copy of that writing shall be retained in the record.

3. Requests for an Accounting.

a) **To be provided to the Victim.** If the victim subsequently requests an accounting of disclosures of PHI, DCG must include an accounting of a disclosure made under this Policy.

b) **To be provided to a Personal Representative.** If the request for an accounting is made by the victim's Personal Representative and DCG:

1. Reasonably believes that the person is responsible for the abuse, neglect, or other injury, or that treating that person as a personal representative could endanger the victim, and

2. In the exercise of professional judgment, decides that informing that person about a report under this Policy would not be in the best interest of the victim, then DCG does not have to treat that person as the Personal Representative and should not provide an accounting of a disclosure under this Policy.

5. Disclosures made under this Policy shall be made pursuant to DCG's Accounting of Disclosures P&S Policy, and retained for six (6) years.

HIPAA PRIVACY POLICIES:
USE AND DISCLOSURE OF PHI

Topic: MINIMUM NECESSARY

Date Adopted: 3/17/2020

I. POLICY

DCG makes reasonable efforts to limit the PHI to the "*Minimum Necessary"* to accomplish the intended purpose of any use, disclosure or request as required by HIPAA, HITECH and other applicable laws and DCG's P&S Policies.

This Minimum Necessary standard applies to all uses and disclosures of PHI permitted by HIPAA except:

(1) Disclosures to or requests by a health care provider for ***treatment***;
(2) Uses or disclosures made **to the Patient**;
(3) Uses or disclosures made **pursuant to a Patient Authorization**;
(4) Disclosures made to the **Department of Health and Human Services**;
(5) Uses or disclosures that are **required by law**; or
(6) Uses or disclosures that **are required for compliance** with DCG's P&S Policy.

II. PROCEDURES

1. DCG will require its employees, agents and other workforce members to use and disclose only the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request. DCG will assess and implement reasonable processes to safeguard a Patient's entire medical record from access except where specifically justified by the circumstances such as for treatment purposes (e.g., filters for medication or allergies, and implementation of role-based access controls).

2. DCG will require its Business Associates, agents and subcontractors to limit use and disclosure to the minimum necessary to accomplish the intended purpose, subject to any guidance made available and applicable by the Secretary of the Department of Health and Human Services.

3. In the event DCG is acting on behalf of a Covered Entity as a Business Associate, DCG will comply with the terms of the respective BAA and HIPAA in determining the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

4. To the extent practicable, with respect to the use, disclosure, or request of PHI, DCG will require the amount of PHI used, disclosed or released limited to:

   (a) the Limited Data Set for such PHI, which shall exclude the following direct identifying information of the Patient or of relatives, employers, or household members of the Patient:

      (1) Names;

(2) Postal address information, other than town or city, State, and zip code.;
(3) Telephone numbers;
(4) Fax numbers;
(5) Electronic e-mail addresses;
(6) Social security numbers;
(7) Medical record numbers;
(8) Health plan beneficiary numbers;
(9) Account numbers;
(10) Certificate/license numbers;
(11) Vehicle identifiers and serial numbers, including license plate numbers;
(12) Device identifiers and serial numbers;
(13) Web Universal Resource Locators (URLs);
(14) Internet Protocol (IP) address numbers;
(15) Biometric identifiers, including finger and voice prints; and
(16) Full face photographic images and any comparable images;

OR

(b) the Minimum Necessary amount of PHI to accomplish the intended purpose of the use, disclosure, or request.

5. If any request for, or use of PHI by, another person appears to be not warranted or is excessive, the concerned employee may consult with the requester or the Patient to determine whether the scope of the request is accurate and/or consult with the Privacy Officer. In the event an employee cannot resolve the issue informally, the requested information will not be disclosed until the Privacy Officer is consulted for further direction.

6. Upon the issuance of further guidance by the Secretary of Health and Human Services regarding implementation of the requirements for Minimum Necessary, DCG will update this Policy accordingly.

HIPAA PRIVACY POLICIES:
USE AND DISCLOSURE OF PHI

Topic: REASONABLE SAFEGUARDS

Date Adopted: 3/17/2020

I. POLICY

DCG will implement reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of PHI. DCG will (i) implement reasonable safeguards to protect PHI from any intentional or unintentional use or disclosure that is in violation of DCG's P&S Policies, and; (ii) limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure. Notwithstanding the procedures set forth in this Policy, DCG will implement such additional reasonable and appropriate administrative, technical and physical safeguards as required under the HIPAA Security Rule and related DCG P&S Policies with respect to electronic PHI ("ePHI").

II. PROCEDURES

1. DCG will use reasonable efforts to limit the information used or disclosed by its employees and other workforce members and agents to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

2. DCG will use reasonable efforts to protect PHI in any form or format and keep such PHI confidential at all times, unless such use or disclosure is permitted under DCG's P&S Policies or applicable law.

3. When using or disclosing a Patient's Social Security Number, all employees must act in compliance with DCG's Social Security Numbers Policy and Procedures.

4. All employees must keep conversations concerning PHI to a minimum while in public places or where such conversations could be overheard by unauthorized individuals.

5. All employees should ensure that computer monitors are turned away from public view. DCG will additionally safeguard computers through which PHI may be accessed in accordance with its Security Policies.

6. Computer usernames and passwords will be assigned to each individual authorized to access PHI and employees, agents and other workforce will be required to keep such log-in information confidential.

7. Business Associate Agreements will be entered into with all persons/entities who need access to PHI to perform a function on behalf of DCG as required by DCG's Business Associates P&S Policy. Copies shall be retained for six (6) years from the date on which such Agreement expires or terminates.

8. All file cabinets and offices containing paper PHI, Social Security Numbers and other confidential information must be kept secured, and personnel with access to such records limited.

9. The identity and authority of requesting individuals and entities will be verified by each employee or other workforce member prior to granting access to, disclosing or making available copies of PHI. to such individual or entity

10. Documents and removable media containing PHI, including Social Security Numbers, must be **shredded, incinerated or disintegrated** prior to disposal in accordance with DCG's Disposal of PHI and ePHI Policy.

11. Employees must take care that any **Social Security Numbers** printed on mailings are not printed on a postcard or external envelope or otherwise readily visible without having to open the envelope.

HIPAA PRIVACY POLICIES:
USE AND DISCLOSURE OF PHI

Topic: WORKFORCE ACCESS TO MEDICAL RECORDS

Date Adopted: 3/17/2020

I. POLICY

DCG prohibits employees, agents and workforce members from accessing their own medical record maintained in DCG's electronic medical record ("EMR"). Employees, agents and workforce members are also prohibited from accessing the EMR of their spouses, children, other family members, friends, colleagues and other individuals unless they are involved in their care and treatment or otherwise specifically authorized to access the EMR in the performance of their job responsibilities. Curiosity viewing is strictly prohibited.

II. PROCEDURES

1. Access to Own EMR. Employees, agents and workforce members may not access or view PHI and other information maintained by DCG about them directly in the EMR. Requests for access to or copies of the workforce member's PHI which may be maintained by DCG concerning the workforce member must follow the same process required for patient requests to access or view PHI.

2. Access to Family Member and Other Individual EMR. Employees, agents and workforce members are strictly prohibited from accessing or viewing PHI of any family member, friend, colleague or other individual unless such workforce member is directly involved in treatment of such individual or otherwise required to access or view such PHI in the performance of his or her job responsibilities. If a workforce member is not authorized by DCG to treat such individual or otherwise access the EMR concerning such individual, the workforce member is not permitted to access the EMR/PHI, *even if* the workforce member may independently be involved in the individual's care outside of his or her DCG job functions (i.e., as a caregiver or spouse). Access to the EMR without authorization is a violation of DCG's P&S Policies and a violation of HIPAA. Requests for access to or copies of family member PHI must follow the same process required for patient requests to access or view PHI.

3. No Curiosity Viewings. DCG will not tolerate "curiosity viewings" (i.e., "checking in" on a neighbor or colleague, celebrity viewings). DCG reserves the right to conduct routine and periodic auditing of all workforce member accesses to the DCG EMR in accordance with applicable DCG P&S Policies. Violations of this Policy will result in disciplinary action in accordance with DCG's Sanction and related HR Policies.

4. HIPAA Responsibility. Individuals may be held individually responsible for violations of HIPAA, including but not limited to the following. Violations may be punishable by applicable

governmental authorities and may include civil fines and/or imprisonment, depending on the severity.

(a) Knowingly accessing, using or disclosing PHI without authorization;
(b) Accessing, using or disclosing PHI under false pretenses;
(c) Accessing, using or disclosing PHI, including selling PHI, for commercial gain, personal gain or malicious harm.

HIPAA PRIVACY POLICIES:

SPECIAL CATEGORIES OF INFORMATION

Topic: HIV-AIDS INFORMATION

Date Adopted: 3/17/2020

I. POLICY

Any and all PHI which contains identifying information about an Individual who has or is suspected of having Acquired Immune Deficiency Syndrome ("AIDS") or HIV (which means an infection with the human immunodeficiency virus or any other related virus identified as a probable causative agent of AIDS) (collectively, the "HIV/AIDS Records") should be maintained in the highest of confidence. The limits placed by this Policy on disclosures of HIV/AIDS Records will continue to apply for as long as such records are maintained by DCG or by a Business Associate on behalf of DCG.

II. PROCEDURES

1. Written Consent Required. Specific informed written consent of the Individual is required prior to any episodic use and disclosure of HIV/AIDS Records, except for the limited treatment purposes as described in the next paragraph. Such form of consent must comply with the requirements for written consent set forth in 42 CFR Part 2.

2. Written Consent Not Required. HIV/AIDS Records may be disclosed without written consent only under the following limited conditions:

    (a) To qualified personnel for the purpose of conducting **scientific research**, but a record shall be released for research only following review of the research protocol by an Institutional Review Board constituted pursuant to federal regulation 45 CFR § 46.101 et seq. Note that the Individual who is the subject of the record shall not be identified, directly or indirectly, in any report of the research and research personnel shall not disclose the Patient's identity in any manner;

    (b) To qualified personnel for the purpose of conducting **management audits, financial audits or program evaluation**, but the personnel shall not identify, directly or indirectly, the Individual who is the subject of the record in a report of an audit or evaluation, or otherwise disclose the Patient's identity in any manner. Identifying information shall not be released to the personnel unless it is vital to the audit or evaluation;

(c) To qualified personnel involved in **medical education or in the diagnosis or treatment of the person** who is the subject of the record. Disclosure is limited to personnel directly involved in the medical education or in the diagnosis and treatment of the person;

(d) To the **New Jersey Department of Health** as required by State or federal law;

(e) As permitted by **rules and regulations adopted by the New Jersey Commissioner of Health** for the purposes of disease prevention and control;

(f) In all other instances **authorized by State or federal law**; or

(g) By **court order** which is granted pursuant to an application showing "good cause."

3. Deceased or Incompetent Individuals. Where the Individual is deceased or incompetent, consent may be obtained from:

   (a) An executor, administrator or authorized representative;

   (b) A spouse, domestic partner, primary caretaking partner, or, if none, from another member of the Patient's family;

   (c) If no next-of-kin or authorized representative, from the Commissioner of the New Jersey Department of Health.

4. Prior to disclosing HIV/AIDS Records without a Patient's prior written consent as may be permitted by this Policy and Procedures, all employees, agents and other workforce members shall notify and consult with the Privacy Officer. In any matter referred to or otherwise being resolved by the Privacy Officer, the Privacy Officer together with legal counsel will evaluate the request for PHI in light of all relevant policies and laws, and shall determine whether the disclosure of the PHI may be made.

5. All requests for or disclosures of HIV/AIDS Records under this Policy will be documented, along with the actions taken to determine whether the disclosure could be made, DCG's decision regarding the request and, if a disclosure was made, a description in the log in accordance with DCG's Accounting of Disclosures P&S Policy. Such documentation shall be maintained for a period of six (6) years.

HIPAA PRIVACY POLICIES:

SPECIAL CATEGORIES OF INFORMATION

Topic: SEXUALLY TRANSMITTED DISEASES

Date Adopted: 3/17/2020

I. POLICY

DCG will implement reasonable safeguards to protect the confidentiality of information related to an Individual who has or who is suspected of having a sexually transmitted (venereal) disease and not disclose such information for any reason other than as may be permitted by law unless DCG obtains the specific authorization of the Individual prior to the disclosure.

II. PROCEDURES

1. The name, address or identity of any person known or suspected to have a venereal disease may not disclosed without the Patient's specific informed consent.

2. In the event Provider does not obtain the Patient's specific informed consent, any information related to whether an Individual has a venereal disease may only be disclosed:

   (a) To the Patient's **treating physician**;

   (b) To the **New Jersey Department of Health** or other health authority as required for the reporting of communicable diseases.

   (c) In the **event of prosecution**, to a prosecuting officer or the court; *provided that* the person's physician or a health authority, when and only when, deems such disclosure necessary to protect the health or welfare of the person, his family or the public.

   (d) Documents, records or reports containing such information may be inspected in connection with any claim for compensation or damages for personal injury or death resulting from the prosecution referenced above by any person authorized by any other law to make such examination.

3. Nothing in this Policy shall prevent a physician from disclosing information regarding venereal diseases to the State Department of Health or local board of health as required by N.J.S.A. 26:4-15.

4. All requests for or disclosures under this Policy must be documented, along with the actions taken to determine whether the disclosure could be made, DCG's decision regarding the request and, if a disclosure was made, a description in the log in accordance with DCG's Accounting of Disclosures P&S Policy. Such documentation must be maintained for a period of six (6) years.

HIPAA PRIVACY POLICIES:

SPECIAL CATEGORIES OF INFORMATION

Topic: DRUG & ALCOHOL TREATMENT INFORMATION

Date Adopted: 3/17/2020

I. POLICY

DCG implements reasonable and appropriate safeguards to maintain any and all PHI which contains identifying information regarding the diagnosis, prognosis or treatment of an Individual for alcohol and/or drug abuse, which is received, directly or indirectly, from a **federally regulated or assisted drug or alcohol treatment facility** (collectively, the "Alcohol/Drug Abuse Records") in the highest confidence. The limits on disclosure of Alcohol/Drug Abuse Records as described in this Policy will continue to apply for as long as such information is maintained by DCG or by a Business Associate on behalf of DCG.

II. PROCEDURES

1. Prior Written Consent Needed. Alcohol/Drug Abuse Records may not be disclosed for any reason other than may be permitted by law, unless the specific informed written consent of the Individual, who is the subject of the Alcohol/Drug Records, is obtained prior to the disclosure. Such consent shall comply at all times with the requirements of HIPAA and 42 CFR Part 2. **DCG's HIPAA Authorization to Use and Disclose PHI is NOT a valid consent for purposes of 42 CFR Part 2.**

2. Prior Written Consent Not Needed. In the event the prior written consent of such Individual is not obtained, the Alcohol/Drug Records may only be disclosed under the following limited conditions, *even if such disclosure would be permissible under HIPAA and state law*:

    (a) To medical personnel to the extent necessary to meet a bona fide medical emergency;

    (b) To qualified personnel for the purpose of conducting scientific research, management audits, financial audits, or program evaluation, but such personnel may not identify, directly or indirectly, any Individual in any report of such research, audit, or evaluation, or otherwise disclose Individual identities in any manner; or

    (c) If authorized by an appropriate court order of competent jurisdiction, granted after an application showing good cause.

3. Except for disclosure by court order, Alcohol/Drug Abuse Records may not be used or disclosed (without a Patient's prior written consent), to initiate or substantiate any criminal charges against an Individual or to conduct any investigation of an Individual.

4. **This Policy does not apply to alcohol/drug abuse records that were not maintained in connection with a federally regulated or assisted drug or alcohol treatment program or facility subject to Part 2. This Policy also does not apply to minor drug & alcohol treatment information.** See Provider Minors Policy & Procedures for specific procedures for minor drug & alcohol treatment information.

5. The foregoing restrictions are not meant to prevent an Individual from accessing his or her own records, including the opportunity to inspect and copy any records that DCG or its Business Associates maintain about the Individual.

6. Each and every disclosure of Alcohol/Drug Abuse Records maintained in connection with a **federally regulated or assisted drug or alcohol treatment facility or program** that is made with the Patient's written consent must be accompanied by the following written statement:

NOTICE TO RECIPIENT OF INFORMATION

"THIS INFORMATION HAS BEEN DISCLOSED TO YOU FROM RECORDS PROTECTED BY FEDERAL CONFIDENTIALITY RULES (42 CFR PART 2). THE FEDERAL RULES PROHIBIT YOU FROM MAKING ANY FURTHER DISCLOSURE OF THIS INFORMATION UNLESS FURTHER DISCLOSURE IS EXPRESSLY PERMITTED BY THE WRITTEN CONSENT OF THE PERSON TO WHOM IT PERTAINS OR AS OTHERWISE PERMITTED BY 42 CFR PART 2. A GENERAL AUTHORIZATION FOR THE RELEASE OF MEDICAL OR OTHER INFORMATION IS NOT SUFFICIENT FOR THIS PURPOSE. THE FEDERAL RULES RESTRICT ANY USE OF THE INFORMATION TO CRIMINALLY INVESTIGATE OR PROSECUTE ANY ALCOHOL OR DRUG ABUSE INDIVIDUAL."

7. Prior to disclosing Alcohol/Drug Abuse Records without a Patient's prior written consent, each employee, agent or workforce member must notify and consult with the Privacy Officer. There are specific requirements under federal law, which govern how disclosures of Alcohol/Drug Abuse Records are to be handled in the event of medical emergencies (e.g., how such disclosures are to be documented); disclosures in the course of audit and evaluation activities (e.g., when Alcohol/Drug Abuse Records may be copied or removed); and presentment of a court order (e.g., whether Provider should comply with court order. Note that a court order does not compel disclosure, unless a subpoena or other similar legal mandate is issued to compel disclosure).

8. In any matter referred to or otherwise being resolved by the Privacy Officer, the Privacy Officer together with legal counsel shall evaluate the request for PHI in light of all relevant policies and laws and determine whether the disclosure of the PHI may be made.

9. DCG will document all requests for Alcohol/Drug Abuse Records, the actions taken to determine whether the disclosure could be made, the decision regarding the request and, if applicable, a description in the log in accordance with DCG's Accounting of Disclosures P&S Policy.

HIPAA PRIVACY POLICIES:

SPECIAL CATEGORIES OF INFORMATION

Topic: GENETIC INFORMATION

Date Adopted: 3/17/2020

I. POLICY

DCG recognizes that genetic information is considered PHI for purposes of HIPAA and HITECH. DCG further requires that genetic information of Patients and employees be obtained, retained and used in strict accordance with the Genetic Information Non-Discrimination Act of 2008 (GINA) and the **New Jersey Genetic Privacy Act.** No *employee* may be discriminated against on the basis of his or her genetic information and an employee or individual's authorization will be required for all uses and disclosures of genetic information unless otherwise permitted by law.

II. PROCEDURES

1. Employees.

   (a) It is against DCG's policy to fail or refuse to hire or discharge any employee or otherwise discriminate any employee with respect to compensation, terms, conditions or privileges of employment as a result of the employee's genetic information.

   (b) DCG will not otherwise limit, segregate or classify employees in any way that would deprive or tend to deprive an employee of an employment opportunity or otherwise adversely affect the status of the employee as a result of the employee's genetic information.

   (c) DCG will not *request, require or purchase genetic information regarding an employee or employee family member **except** for:*

      (1) Where DCG accidentally/inadvertently requests/requires family medical history from the employee or employee family member;

      (2) Where:

         (a) Health or genetic services offered by DCG (e.g., services offered as part of a wellness program);

         (b) Where the employee provides prior, knowing, voluntary, and **written authorization;**

         (c) Where only the employee/employee family member and the licensed health care professional or board certified genetic counselor involved in

providing such services receive the results which contain individually identifiable information; AND

(d) Where individually identifiable genetic information listed above in connection with the health or genetic services offered by Provider *is only available for purposes of such services and shall not be disclosed to the employer <u>except</u> in aggregate terms without disclosing the identity of specific employees.*

(3) Where an employee requests or needs family medical history in accordance with the Family and Medical Leave Act of 1993 or the New Jersey Family Leave Act;

(4) Where DCG purchases documents commercially and publically available (newspapers, magazines, etc) with family medical history;

(5) Where the information is to be used for *genetic monitoring* of biological effects of toxic substances in the workplace, but only if:

(a) DCG provides written notice;

(b) Employee provides prior, knowing, voluntary <u>and</u> written authorization <u>OR</u> genetic monitoring is required by federal or state law;

(c) The employee is informed of individual monitoring results;

(d) Monitoring is in compliance any state or federal genetic monitoring regulations;

(e) DCG, except any licensed health care professional or board certified genetic counselor, receives results in only *aggregate terms;*

(6) Where DCG conducts DNA analysis for law enforcement purposes as a forensic laboratory or to identify human remains identification.

(d) DCG will maintain any genetic information it possesses concerning employees in a **<u>separate medical record and location</u>** from other medical and employment records and shall treat such information as a confidential medical record. Any DNA samples obtained for employment purposes must be destroyed promptly unless retention is authorized by law.

(e) DCG may not <u>disclose</u> any genetic information concerning an employee <u>except:</u>

(1) As may be permitted by HIPAA (e.g., for treatment, payment and health care operations)

(2) To the employee (or family member where the family member received the service) at the *written request* of the employee;

(3) To an occupational or other health researcher where the research is conducted in accordance with part 46 of title 45, CFR.

(4) By court order, and only to the extent expressly authorized by such order, and provided that the employee is notified of the order and any genetic information subsequently disclosed;

(5) To government officials to investigate compliance with genetic privacy requirements;

(6) To the extent the disclosure is made in connection with employee's compliance with the Family and Medical Leave Act of 1993 or New Jersey Family Leave Act;

(7) To a federal, state or local public health agency concerning a contagious disease presenting *imminent hazard of death or life-threatening illness,* and the employee whose family members are subject of a disclosure is notified.

2. Patients and Individuals in General.

(a) *Obtaining Genetic Information.* DCG will not obtain genetic information from a Patient/Individual without his or her *informed written consent*, including for purposes of life insurance policies or disability income insurance contracts. In the event DCG does not obtain consent from the Individual or representative of the Individual, DCG may obtain genetic information only where genetic information is obtained:

(1) By a state, county, municipal or federal law enforcement agency in the course of a criminal investigation or prosecution to establish identity of a person;

(2) To determine paternity in accordance with N.J.S.A. 9:17-48;

(3) Pursuant to the "DNA Database and Databank Act of 1994";

(4) For anonymous research, where the identity of the Individual will not be released;

(5) For newborn screening requirements of state or federal law;

(6) As authorized by federal law to identify persons.

(b) *Retaining Genetic Information.* DCG will not retain genetic information of an Individual without his or her *informed written consent*. In the event DCG does not obtain consent from the Individual or representative of the Individual, DCG may retain genetic information only where genetic information is retained:

(1) As necessary for a criminal or death investigation, or criminal or juvenile proceeding;

(2) As necessary to determine paternity in accordance with N.J.S.A. 9:17-48;

(3) As authorized by the court;

(4) Pursuant to the "DNA Database and Databank Act of 1994";

(5) For anonymous research, where the identity of the Individual will not be released;

(c) *Destroying Genetic Information.* DCG will require that any DNA sample of an Individual destroyed promptly at the request of the Individual or Patient's representative unless:

(1) Retention would be necessary for a criminal or death investigation or criminal or juvenile proceeding; or

(2) Retention is authorized by the court.

DNA samples from Individuals in research projects shall be destroyed *automatically* unless the Individual directs otherwise by informed consent.

(d) *Disclosing Genetic Information.* DCG will not disclose genetic information that would permit identification of an Individual, or the identity of an Individual upon whom a genetic test has been performed. In the event DCG does not obtain consent from the Individual or representative of the Individual, DCG may only disclose genetic information without the individual's written consent where necessary:

(1) For purposes of a criminal or death investigation or criminal or juvenile proceeding;

(2) To determine paternity in accordance with N.J.S.A. 9:17-48;

(3) Authorized by the court;

(4) Pursuant to the "DNA Database and Databank Act of 1994";

(5) For purposes of furnishing genetic information related to a decedent for medical diagnosis of blood relatives of the decedent;

(6) For purpose of identifying bodies;

(7) For purposes of newborn screening requirements;

(8) Where authorized by federal law for identification of persons.

3. Notice. Where DCG is authorized by law and this Policy to perform genetic testing or receive records, results or findings of genetic testing, the Individual will be notified that such test was performed or that the results, records or findings were received unless the individual has given written informed consent otherwise. The notice must state that Information regarding the genetic testing or records, results or findings of the genetic testing will not be disclosed to any person without the Patient's written consent, unless DCG is permitted to disclose such information by law. **Notice does not need to be provided to individuals for purposes of newborn screening requirements.**

4. DCG does not need to obtain a parent's informed consent prior to testing newborns pursuant to state newborn screening requirements, if applicable. However, DCG must obtain a parent's informed consent prior to any other disclosure of genetic information related to such screenings for disclosures other than to the New Jersey Department of Health and Senior Services or other agency designated by law to receive such newborn screening results.

5. **This Policy does not prohibit the use, acquisition or disclosure of medical information that is *not* genetic information (e.g., a manifested disease, disorder or pathological condition that may have a genetic basis).**

6. All requests for genetic information will be documented, including the actions taken to determine whether the disclosure could be made, the decision regarding the request and, if a disclosure was made, a description in the log in accordance with DCG's Accounting of Disclosures P&S Policy. All documentation shall be retained for a period of six (6) years.

HIPAA PRIVACY POLICIES:

SPECIAL CATEGORIES OF INFORMATION

Topic: MINORS

Date Adopted: 3/17/2020

I. POLICY

In general, DCG may disclose PHI regarding a minor Individual ("Minor Records") to the minor Patient's parent, guardian, or other person acting *in loco parentis* (collectively, the "Parent"), and may treat the Parent as the minor's "personal representative" with respect to the Minor Records relevant to such personal representation. However, in certain situations, where minors are authorized under applicable law to consent to a particular health care service, DCG does not treat the Parent as the personal representative, and the minor (**not** the Parent) may consent to and authorize any use and disclosure of their Individual information.

DCG recognizes that under New Jersey law, minors can consent to and authorize disclosure of their Minor Records if:

(1) Married;
(2) Pregnant (and seeking health care services related to the pregnancy or the minor Patient's child);
(3) Being treated for Alcohol or Drug Use/Abuse;
(4) Being treated for Venereal Disease or Sexual Assault*;
(5) The minor is 12 years old or older, and his or her Individual information relates to AIDS or HIV infection**;
(6) The minor is 14 years old or older, and is admitted to a psychiatric facility, children's crisis intervention service or special psychiatric hospital operated by a state-licensed mental health provider; or
(7) Emancipated (18 years old or older).

DCG will routinely check for any changes in state law with respect to the foregoing.

II. PROCEDURES

1. Employees, agents and other workforce will assess whether the Minor has sought medical treatment independently with authority under State law, and whether the Minor must be treated as the Individual with authority to control access and disclosure to his or her PHI prior to disclosing Minor Records to a Parent without a minor Patient's prior written consent.

2. The Minor Patient's treating physician will be consulted with to assess whether information regarding the Minor's treatment and/or the Minor's Records should be withheld or provided to a Parent.

3. The Minor's treating physician (and Privacy Officer, as necessary) will evaluate the request for the Minor's Records in light of all relevant policies and laws, and shall determine whether the disclosure of PHI may be made. However, the decision to provide or deny access to Information to a parent, guardian or other custodian regarding a Minor's Treatment is ultimately made by the **Minor's treating physician**, in the exercise of **professional judgment**. This means that the treating physician of the Minor Individual **may** (but is not required to) in his/her discretion:

    (a) Not treat the Parent as the personal representative of the Minor Individual;

    (b) Deny the Parent access to Information about the Minor's Treatment; or

    (c) Inform the Parent of the Minor Patient's treatment for health care services (including treatment for venereal disease and alcohol/drug abuse), even over the Minor's **express refusal**. Note that with respect to cases of sexual assault, the Parent must be notified immediately, unless the treating physician believes it is in the best interests of the minor Individual not to do so.

4. All requests for a Minor's Records or related information under this Policy will be documented, including the actions taken to determine whether the disclosure could be made, the decision regarding the request and, if a disclosure was made, a description in the log in accordance with DCG's Accounting of Disclosures P&S Policy.

** Note that with respect to Minor Records related to AIDS or HIV infection, conflicting regulations place the age of consent at 12 years old. Additionally, New Jersey law requires that "when consent is required for *disclosure* [emphasis added] of the record of a minor who has or is suspected of having AIDS or HIV infection, consent shall be obtained from the parent, guardian or other person authorized under State law to act on the minor's behalf." N.J.S.A. 26:5C-13.

HIPAA PRIVACY POLICIES:

SPECIAL CATEGORIES OF INFORMATION

Topic: SOCIAL SECURITY NUMBERS

Date Adopted: 3/17/2020

I. POLICY

Individual Social Security Numbers must be kept confidential to protect the privacy and security of Individuals and comply with the New Jersey Identity Theft Prevention Act, N.J.S.A. 56:11-44 et seq., HIPAA, and other federal and state laws and regulations.

II. PROCEDURES

1. When it comes to a Patient's Social Security Number, employees, agents and other workforce members shall **NOT**:

    (a) Print a SSN on any mailings unless required by state or federal law;
    (b) Posted or publicly display an individual's SSN (whether in full or any four or more consecutive numbers of the individual's Social Security number);
    (c) Print a SSN on any card required for access to products or services provided by SSN;
    (d) Require the SSN to be transmitted over the Internet without an accompanying password or unique PIN or other authentication device;

2. A Patient's Social Security Number may be used as permitted below:

    (a) Where otherwise permitted by state or federal law;
    (b) For internal verification and administrative purposes, so long as the use does not require release of the Social Security Number to unauthorized individuals;
    (c) In applications and forms sent by mail, including where part of an enrollment process or to establish, amend or terminate an account, contract or policy, or confirm the accuracy of the Social Security Number, HOWEVER, such Social Security Number may not be printed on a postcard or mailer not requiring an envelope nor where it would be visible on the envelope;
    (d) Otherwise temporarily cache or store, transmit or route an image, information or data concerning the number;

3. Where requesting a Patient's Social Security Number, the individual must be informed, upon request, of the reason it has requested the Social Security Number. Employees, agents and other workforce members must at all times maintain the confidentiality of the Social Security Number unless would otherwise be permitted to do so by law.

HIPAA SECURITY POLICIES:

ADMINISTRATIVE SAFEGUARDS

Topic: SECURITY MANAGEMENT PROCESS

Date Adopted: 3/17/2020

I. POLICY

DCG strives to prevent, detect, contain and correct all security violations through:

- Performing a Gap and Risk Assessment to evaluate potential risks and vulnerabilities to confidentiality integrity and availability of e-PHI **(*Required*);**
- Implementing security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level **(*Required*);**
- Applying sanctions against workforce who fail to comply with security policies and procedures **(*Required*);** and
- Implementing procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports **(*Required*).**

II. PROCEDURES

1. The Security Officer and/or his or her designees will identify relevant information systems that store e-PHI/Data, either temporarily or permanently, including all hardware and software that are used to collect, store, process, or transmit e-PHI/Data. The results of such inventory will be documented and maintained by the Security Officer for a period of at least six (6) years from the date of the performance of such inventory, along with any methods for tracking such inventory.

2. Business functions will be analyzed and ownership and control of information system elements verified as necessary. The following should be considered:

   (a) Who or what organization is responsible for the specific hardware or software?

   (b) Whether the current information system configuration is documented, including connection to other systems?

   (c) Have the types of information and uses of that information been identified and the sensitivity of each type of information been evaluated? Each type of Data should be **classified** with regard to its impact on business operations (essential or **critical vs. non-essential**), level of security or **threat risk,** and/or proprietary or **confidential** nature.

(d) Is access to such Data limited to what is reasonable and necessary given the nature of each type of Data's classification and reasonable and appropriate safeguards applied to prevent unauthorized access?

3. **For any portable devices and media, such as mobile devices and laptops, which may have access to or maintain PHI, the Security Officer will, as appropriate, consult guidance made available by the Office for Civil Rights prior to permitting any PHI to be accessed, created, maintained or transmitted through such:**

   http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

4. The Security Officer will conduct a Gap and Risk Assessment (See "Security Gap and Risk Assessment" Tool) on a routine basis and periodically as may be appropriate and determined by the Security Officer, in accordance with DCG's Risk Assessment and Information Systems Activity Review P&S Policies.

5. The Security Officer will document output and outcomes from the risk assessment. Documentation will be retained for a period of six (6) years. Risk assessments will be reviewed periodically as reasonably necessary to ensure any identified deficiencies or security measures have been resolved or are in the processes of resolution.

6. The Security Officer will monitor the performance, access to, and use of all information systems, and assess periodically whether additional hardware, software and/or services may be needed to reasonably and adequately protect e-PHI/Data. If "yes," the Security Officer will make reasonable and appropriate selections, and modifications taking into consideration (1) applicability of the IT solution to the environment (2) sensitivity of data (3) DCG's Security Policies, procedures and standards (4) resources available for operation, maintenance and training (5) appropriate access to and use of Data.

7. The Security Officer will document all decisions concerning the management, operational, and technical controls selected to identify, evaluate and mitigate identified risks. Documentation will be retained for a period of six (6) years.

8. The Security Officer will establish roles and responsibilities for the implementation of each control to particular individuals or offices.

9. The Security Officer will develop and implement procedures as reasonably necessary to accomplish particular security related tasks necessary and appropriate for DCG's business operations.

HIPAA SECURITY POLICIES: ADMINISTRATIVE SAFEGUARDS

Topic: ASSIGNED SECURITY RESPONSIBILITY

Date Adopted: 3/17/2020

I. POLICY

DCG will designate a HIPAA Security Officer as responsible for developing, implementing, monitoring and assuring enforcement of DCG's HIPAA Policies and Procedures. DCG will identify and select an individual who is capable, together with his or her designees, of assessing, implementing and evaluating effective security policies and procedures to safeguard the confidentiality, integrity and availability of ePHI and other Data maintained, created or received by DCG, including those privacy policies and procedures necessary for DCG to comply with the requirements of HIPAA, HITECH and other applicable state and federal law.

II. PROCEDURES

1. DCG will select and approve an individual who is able to assess effective HIPAA security and to serve as the point of contact for security policy, implementation, and monitoring.

2. DCG will adopt a resolution appointing the individual, which resolution is signed by the governing body of DCG, as may be applicable.

3. DCG will clearly document the Security Officer's responsibilities in a written job description reflecting assigned security duties and responsibilities of the security official, and attach such to this Policy as Exhibit "A". Such written job description will be periodically reviewed by DCG and amended as reasonable and appropriate.

4. The Security Officer will be responsible for implementing and appointing the HIPAA Security Policies and Procedures, and managing all information systems, developing and implementing such security controls and other procedures reasonable and appropriate for safeguarding the confidentiality, integrity and availability of PHI and other Data. The Security Officer will be responsible for appointing appropriate workforce members as necessary for the management and implementation of these HIPAA Policies and Procedures, and designating individuals to act on his or her behalf with regard to such.

5. DCG will make the identity of the appointed Security Officer known to the entire organization so that employees and other workforce members at DCG are aware of whom to contact in the event of a HIPAA privacy or security problem or other security concerns.

EXHIBIT B

JOB DESCRIPTION - HIPAA SECURITY OFFICER

1. Overview.

The HIPAA Security Officer is responsible for Organization's HIPAA Security Rule compliance, including, but not limited to, overseeing and ensuring development, implementation, and maintenance of DCG's HIPAA Security Rule policies and procedures, monitoring compliance with the HIPAA Security Rule, and investigation and remediation of security breaches affecting electronic protected health information ("**e-PHI**").

2. Responsibilities:

The HIPAA Security Officer:

- Works together with DCG's HIPAA Privacy Officer to develop a strategic and comprehensive "**HIPAA Program**" which ensures DCG's compliance with HIPAA, the Security Rule, and other HIPAA-implementing regulations.
- Ensures defining, development, implementation and maintenance of policies and processes which enable consistent, effective practices that minimize risk and ensure the security of e-PHI across all media.
- Ensures all forms, policies, standards, and procedures for DCG's HIPAA Program are up-to-date with HIPAA, the HIPAA Security Rule, applicable federal and state laws governing security, and IT security best practices.
- Works together with DCG's HIPAA Privacy Officer, senior management, legal and the Board of Directors to establish governance for DCG's HIPAA Program.
- Collaborates with DCG's HIPAA Privacy Officer to ensure alignment between security and privacy compliance programs including policies, practices, investigations, and acts as a liaison between information systems (IS), compliance and legal personnel or workforce.
- Establishes an ongoing process to audit, track, investigate and mitigate security incidents, and any unauthorized access and disclosure of e-PHI. Monitor patterns of unauthorized access and/or disclosure of e-PHI.
- Performs initial and periodic information HIPAA Risk Analysis, gap mitigation and remediation as required by the HIPAA Security Rule.
- Conducts related ongoing compliance monitoring activities in coordination with DCG's other compliance and operational assessment functions.
- Takes a lead role, to ensure DCG has and maintains appropriate administrative, physical and technical safeguards reflecting DCG's current HIPAA security practices and requirements.
- Oversees, develops and delivers initial and ongoing HIPAA Security training, education and "Security Reminders" for DCG "Workforce".
- Works together with the HIPAA Privacy Officer in the development, implementation, and ongoing compliance monitoring of all DCG vendors who may handle e-PHI on

behalf of DCG, including ensuring that HIPAA BA Agreements are executed and enforced. Ensuring Business Associate HIPAA security concerns, requirements, and responsibilities are addressed.

- Coordinates and oversees the security component of any HIPAA Breach or Security Incident evaluation and determination. Coordinates and together with the HIPAA Privacy Officer completes any required HIPAA Breach Risk Assessment, documentation, and mitigation of Security Incidents and Breaches. Works with Human Resources to ensure consistent application of sanctions for HIPAA Security Rule violations.
- Establishes and administers a process for investigating and acting on HIPAA Security complaints, and work together with DCG's Privacy Officer to respond to complaints concerning security.
- Initiates, facilitates and promotes activities to foster HIPAA Security awareness within DCG and its various programs.
- Maintains current knowledge of HIPAA and other applicable federal and state security laws and accreditation standards.
- Works with DCG administration, legal counsel, and other related parties to represent DCG's HIPAA Security interests with external parties (state or local government bodies) who undertake to adopt or amend legislation, regulation, or standard which may affect the Security of DCG's HIPAA Program.
- Cooperates with the U.S. Department of Health and Human Service's Office for Civil Rights, State regulators and/or other legal entities in any HIPAA Security Rule related compliance reviews or investigations.
- Serves as HIPAA Security resource to DCG and all DCG employees, agents, and other workforce regarding the security and safeguarding of all e-PHI, and all HIPAA Security-related issues.
- Such other duties and responsibilities in order for DCG to fully meet the requirements of HIPAA.

HIPAA SECURITY POLICIES:

ADMINISTRATIVE SAFEGUARDS

Topic: RISK ASSESSMENTS

Date Adopted: 3/17/2020

I. POLICY

DCG conducts routine and periodic risk assessments/analyses of the potential risks, threats and vulnerabilities to the confidentiality, integrity, and availability of electronic Protected Health Information ("ePHI") it may create, receive, maintain or transmit as a Covered Entity.

II. PROCEDURES

1. Responsibility for conducting periodic Risk Assessments will be with the designated HIPAA Security Officer, who will establish a plan and procedures for the conduct of such Risk Assessments.

2. All such Risk Assessments will be conducted periodically in response to environmental or operational changes that may affect PHI, and *routinely* in accordance with such timeframe as determined to be appropriate by the Security Officer.

3. The Risk Assessment process should be, to the extent practicable, modeled upon the risk analysis process recommended by the National Institute for Standards and Technology ("NIST"), SP 800-30. DCG will use, as reasonable appropriate, other information technology "Best Practices" to assist in performing the Risk Analyses and other Self-Assessments.

4. The results of Risk Assessments will become an integral part of management's decision-making process, and will guide decisions related to the protection of PHI. The Security Officer will be responsible for implementing, assessing and modifying security controls in order to response to, correct and/or mitigate any identified security deficiencies and gaps. All results of Risk Assessments should be reviewed and re-assessed on a periodic basis by the Security Officer as part of ongoing Security Risk Management.

5. All such risk analyses and assessments will be maintained and documented for a period of at least six (6) years from the date on which the Risk Assessment was performed. A copy of the two (2) most recent risk analyses results/review of risk analyses will be maintained as an attachment to this Policy.

HIPAA SECURITY POLICIES:

ADMINISTRATIVE SAFEGUARDS

Topic: INFORMATION SYSTEMS ACTIVITY REVIEW

Date Adopted: 3/17/2020

I. POLICY

DCG regularly reviews various indicators and records of information system activity, including, but not limited to: audit logs; access reports; and security incident reports. DCG strives to prevent, detect, contain, and correct security violations and threats to PHI, whether in electronic or any other forms.

II. PROCEDURES

1. The Security Officer and/or his or her designees will be responsible for implementing processes and procedures to routinely and periodically review system activity logs and reports. The Security Officer together with the HIPAA Privacy Officer will implement audit mechanisms as appropriate to appropriately track activities with regard to PHI in all DCG's information systems which contain, create, transmit or receive PHI.

2. Describe automated audit processes and manual audit processes which will be implemented by Security Officer and/or Privacy Officer, or implemented by Third Party Vendor (i.e., EHR audit processes.

3. The Security Officer will monitor on an ongoing-basis potential threats and vulnerabilities to PHI as well as the continued appropriateness and effectiveness of security controls and safeguards in response to environmental and operational changes.

4. The Security Officer will document all information system activity review activities and efforts and maintain all reports, audit and activity logs generated by systems and/or the Security Officer in connection with the information systems activity review. All reports, audits, activity logs and documented reviews of such will be maintained by DCG for a minimum of six (6) years from the date on which such were generated/reviewed.

5. This Information Systems Activity Review Policy will be implemented and executed in accordance with DCG risk management policies and procedures. The review processes will be reviewed on an ongoing basis and modified as needed to appropriately monitor all IS activity.

HIPAA SECURITY POLICIES:
ADMINISTRATIVE SAFEGUARDS

Topic: STANDARD WORKFORCE SECURITY

Date Adopted: 3/17/2020

I. POLICY

Only members of DCG's workforce who have a need to access e-PHI/Data or certain categories of e-PHI/Data are granted *appropriate* access to e-PHI/Data, and those who do not are prevented from obtaining access. DCG will implement processes to exercise appropriate authorization and supervision over all workforce members and assign and/or terminate access appropriately.

II. PROCEDURES

1. Authorization and Supervision. The Security Officer in connection with respective department directors and management will manage and assign responsibility over and access to PHI and other Data maintained in DCG's information systems and networks through which such PHI and Data is accessed or maintained. The Security Officer will:

    (a) Establish security roles and responsibilities for all job functions.

    (b) Assign each job function the appropriate level and scope of security oversight, training, and access, depending on the responsibilities required of each such function.

    (c) Identify which members of DCG's workforce have the business need, and which have been granted permission, to view, alter, retrieve, and store e-PHI/Data, and at what time, under what circumstances, and for what purposes.

    (d) Ensure appropriate oversight over accesses to and uses of Data, including conducting audits, and modification of such as reasonable and appropriate given workforce job responsibilities and status (i.e., transfer to new department, suspension, leave of absence, termination).

    (e) Contract with information systems and network vendors as may be appropriate to support DCG's workforce security.

    (f) If it is not "*reasonable and appropriate"* to implement procedures allowing for the authorization and/or supervision of workforce members who work with e-PHI/Data or in location where it might be accessed, DCG will **document** the reasons why and a reasonable alternative here:

        - It is not "*reasonable and appropriate"* to implement such procedures because ***(insert description here):***

- The reasonable alternative that will be used to implement such procedures is ***(insert description here***):

2. Workforce Clearance Procedures. The Security Officer, together with department directors and management, will:

   (a) Equip workforce members with necessary knowledge, skills, experience and abilities to fulfill particular roles (e.g., positions involving access to and use of sensitive information).

   (b) Prospective workforce members will be queried with respect to their knowledge and trained on proper uses and disclosures of PHI and DCG's systems.

   (c) Complete employment and educational reference checks, as well as background checks as determined reasonable and appropriate.

   (d) If it is not "*reasonable and appropriate"* to implement procedures allowing for DCG to determine that the access of a workforce member to e-PHI/Data is appropriate, DCG will **document** the reasons why and a reasonable alternative here:

   - It is not "*reasonable and appropriate"* to implement such procedures because (***insert description here)***:

   - The reasonable alternative that will be used to implement such procedures is: (***insert description here):***

3. Termination Procedures. The Security Officer will oversee and manage all access rights to ensure workforce member access is terminated as appropriate. The Security Officer will:

   (a) Develop a standard set of procedures to be followed to recover access control devices (e.g., Identification (ID) badges, keys, access cards, etc.) when employment ends as a result of voluntary termination (e.g., retirement, promotion, change of employment) and involuntary termination (e.g., termination for cause, reduction in force, involuntary transfer, and criminal or disciplinary actions).

   (b) Work with the Privacy Officer and Human Resources to create a standard checklist for items to be completed when an employee leaves. The checklist will include at a minimum: (1) Return of access and other company issued devices; (2) Deactivation of information

systems/network accounts; (3) Delivery of needed data solely under the employee's control; and (4) reminder of continuing confidentiality obligations upon departure.

(c) Ensure that mechanisms are in place to deactivate information system/network accounts (e.g., disable user IDs and passwords).

(d) If it is not *"reasonable and appropriate"* to implement procedures for terminating access to e-PHI/Data when the employment of a workforce member ends, DCG will **document** the reasons why here:

- It is not "*reasonable and appropriate"* to implement such procedures because (***insert description here)***:

- The reasonable alternative that will be used to implement such procedures is (***insert description here)***:

HIPAA SECURITY POLICIES:
ADMINISTRATIVE SAFEGUARDS

Topic: INFORMATION ACCESS MANAGEMENT

Date Adopted: 3/17/2020

I. POLICY

DCG will maintain current policies that determine which workforce members will be assigned access authority to e-PHI.

II. PROCEDURES

1. Access Authorization. The Security Officer together with respective department directors and management will:

   (a) Assess how access to workstations, transactions, programs, processes and other mechanisms will be determined. **For any portable devices and media, such as mobile devices and laptops, which may have access to or maintain PHI, DCG will consult guidance made available by the Office for Civil Rights as may be appropriate prior to permitting any PHI to be accessed, created, maintained or transmitted through such: http://www.healthit.gov/DCGs-professionals/your-mobile-device-and-health-information-privacy-and-security**

   (b) Determine restrictions on access, which should be *identity-based, role-based, location-based, or some combination thereof*, and consistent with other existing management, operational and technical controls;

   (c) Establish standards for granting access. Formal authorization should be obtained from the Security Officer, or her/his designee, before access to sensitive information is granted to any user. Only the minimum necessary e-PHI should be made available to each workforce member based on his/her job requirements and on a need-to-know basis only.

   (d) In addition, the respective department directors and managers will work with the Security Officer to **identify any laws and regulations** which may additionally restrict workforce access to certain Data, such as employee personnel records, employee medical information, and certain PHI.

   (e) If it is not "*reasonable and appropriate"* to implement procedures to govern granting access to e-PHI, DCG will **document** the reasons why and a reasonable alternative here:

      - It is not "*reasonable and appropriate"* to implement such procedures because ***(insert description here)***:

- The reasonable alternative that will be used to implement such procedures is: ***(insert description here)***

2. Access Establishment and Modification. DCG will:

(a) The Security Officer will evaluate access controls already in place or implement new access controls as reasonably appropriate and as needed, both periodically and on a routine basis.

(b) The Security Officer will coordinate with other existing management, operational, and technical controls, such as policy standards and personnel procedures, maintenance and review of audit trails, identification and authentication of users, and physical access controls.

(c) Members of the workforce will receive security training upon hire and will receive at least annual and periodic updates as necessary. Documentation of completion of this training will be maintained by the Security Officer with a copy sent to Human Resources for each workforce member.

(d) If it is not "*reasonable and appropriate"* to implement procedures that establish, document, review and modify a user's right of access to a workstation, transaction, program or process, DCG will **document** the reasons why and a reasonable alternative here:

- It is not "*reasonable and appropriate"* to implement such procedures because: ***(insert description here)***

- The reasonable alternative that will be used to implement such procedures is: ***(insert description here)***

HIPAA SECURITY POLICIES:
ADMINISTRATIVE SAFEGUARDS

Topic: SCOPE OF ACCESS BY MEMBERS OF WORKFORCE

Date Adopted: 3/17/2020

I. POLICY

DCG will reasonably base access to PHI on employee-role, or class of workforce. The types of persons who are to have access to designated categories of information and the conditions, if any, of that access will be in accordance with a Role-Based Access matrix as may be developed by DCG from time to time. Workforce members may only access PHI or certain categories of PHI where access is required in connection with such workforce member's job functions.

II. PROCEDURES

1. DCG will identify and assign **Role-based** and **Task-based Access Rights** to all workforce members or categories of workforce members or other persons under the control of DCG who will need access to PHI to perform their duties. All role-based and task-based decisions must be documented, and should take into consideration the degree of control exercised over the particular workforce member, licensures, training, experience and other factors in assigning access rights to the workforce member.

    (a) *Administrative/Clerical Staff.* Administrative/clerical staff should only be given access for the following functions:

        (1) Routine billing and other administrative and health care operations;

        (2) Entering general patient information (e.g., name, address, telephone, health insurer or payment information);

        (3) Scheduling diagnostic tests;

        (4) Receiving clinical laboratory results and reports;

        (5) Entering and transmitting* electronic prescriptions (eRX) where authorized by a prescribing physician (**Note: for Schedule II-V controlled substances, physician must be in compliance with all DEA regulations for electronic prescribing. Additionally, for these controlled substances, although the staff member may enter the information, the physician must be the one to sign-off on and "transmit" the eRX)*.

DCG will implement reasonable processes to safeguard against administrative/clerical staff members having access to "enter", "send" or otherwise transmit orders for diagnostic or laboratory tests. *Note: Physician should not permit administrative or clerical staff to "enter" any clinical information into a patient record, such as clinical laboratory results and reports, even where the physician would later review and/or sign-off on the information's entry.*

(b) *APNs, RNs, LPNs, PAs*. Licensed healthcare professionals such as advanced nurse practitioners (APNs), registered nurses (RNs), licensed practical nurses (LPNs) and physician assistants (PAs) may be given access to perform functions within the scope of their license to practice. These may include, but are not limited to:

i. Entering and/or transmitting orders for treatments, prescriptions, medical devices, laboratory and diagnostic tests (for APNs and PAs only);

ii. Entering PHI/Data for later transcription (PAs, RNs and LPNs)

iii. Entering (but not transmitting) orders for diagnostic and laboratory tests or otherwise responding to standing or verbal orders from physicians (RNs)

(c) DCG will implement reasonable controls for physician review and sign-offs as appropriate for each access category type. Physicians must sign-off or finalize **all entries** in a patient record unless the author of the entry has independent authority to sign-off or finalize such entry granted by state or federal law.

2. **DCG will implement processes to exercise appropriate oversight and control over any subcontractor or third party vendor which DCG may grant access to PHI, subject at all times to the "Business Associate" P&S Policy.** Third parties may only be granted access to Data as necessary to perform their functions, subject to at all times the HIPAA P&S Policies, and subject to written agreement as required by the "Business Associate" P&S Policy. Third parties will be required to implement reasonable and appropriate administrative, physical and technical safeguards to protect the privacy and security of any Data which they may have access to, including PHI, and that such use and disclosure is limited at all times to those set forth in an applicable HIPAA BAA. The Security Officer will work together with the departments and management to periodically assess the effectiveness of tracking vendor and subcontractor agreements and implement additional management tools as necessary to ensure oversight and accountability.

3. DCG will implement Technical and Administrative Safeguards in accordance with these P&S Policies and HIPAA to safeguard PHI as required under HIPAA.

4. DCG will train workforce members on their level of permissible access to PHI based on job function, both annually and on a periodic basis as needed and appropriate. Workforce members are required to comply at all times with the DCG "Minimum Necessary" P&S Policy when accessing PHI.

5. DCG will enforce and apply sanctions in accordance with DCG's Sanctions P&S Policy for any instances of non-compliance of workforce members with this Policy.

HIPAA SECURITY POLICIES:

ADMINISTRATIVE SAFEGUARDS

Topic: AUTHENTICATION & VERIFICATION OF INDIVIDUALS/ENTITIES REQUESTING PHI

Date Adopted: 3/17/2020

I. POLICY

Prior to making any disclosures of PHI, DCG will require workforce to verify the identity of the person OR entity, as the case may be, requesting the PHI and the authority of such person/entity to have access to the PHI. Documentation, statements or representations, whether oral or written, will be obtained from the person requesting the PHI, when such documentation, statements or representations are a condition of disclosure.

II. PROCEDURES

1. If a request for PHI is made over the **telephone**, employees, agents and other workforce members may release PHI provided the identity and authority of the requestor is verified and the proper documentation, statements or representations are obtained from the requester.

2. If the identity or authority of any person requesting PHI is **not known** to the particular DCG employee, the employee must verify the identity and authority of the requester by alternate means. Verification may be made by requesting certain information assumed to be known only to the individual, such as the individual's driver's license number and a second piece of information, such as date of birth, address or mother's maiden name.

3. Where the person requesting the PHI appears **in person**, request documentation to verify identity. The requesting individual can be asked for one or more of the following. Additional documentation may be verified on a case-by-case basis.
   (a) Photo identification (e.g., driver's license)
   (b) Birth Certificate;
   (c) Passport.

4. If reasonable under the circumstances, DCG may rely on documentation on its face if it meets the applicable requirements. In addition, DCG may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of PHI is to a **public official** or to a person acting on behalf of the public official:

   (a) If the request is made in person, there is presentation of an agency identification badge, other official credentials, or other proof of government status;

   (b) If the request is in writing, the request is on the appropriate government letterhead; or

(c) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

5. Verification of the authority of the requester should also be satisfied prior to permitting such requester to **access** PHI. Specific documentation of authority (e.g., identification as a parent or guardian, appointment as executor or other appropriate relationship to the individual) should be obtained. In the event of any questions regarding the authority or identity of an individual requesting access to PHI, the Privacy Officer should be contacted.

HIPAA SECURITY POLICIES:

ADMINISTRATIVE SAFEGUARDS

Topic: SECURITY AWARENESS & TRAINING

Date Adopted: 3/17/2020

I. POLICY

DCG provides periodic and annual security awareness & training to its workforce members. DCG will ensure all workforce members are appropriately trained in their responsibilities under the DCG HIPAA Security Policies as well as Privacy Policies with respect to ePHI.

II. PROCEDURES

1. The Security Officer will be responsible together with his or her designees for developing, implementing and updating as necessary training resources and materials to educate workforce members on the requirements of the HIPAA Security Rule and the DCG Security Policies, as required by DCG's Training P&S Policy, together with the Privacy Officer.

2. Security awareness and training will include at a minimum;

    (a) *Security Reminders.* The Security Officer will implement processes to provide periodic security reminders to all workforce members as reasonable and appropriate to correct ongoing security concerns, threats, vulnerabilities or violations concerning the confidentiality, integrity and availability of PHI.

    (b) *Password Management.* The Security Officer will provide education to workforce members on appropriate password creation, maintenance and confidentiality, including selecting "strong passwords", not sharing passwords with any workforce member or other individual, and not writing down passwords. Workforce members are responsible for complying with the following:
        (i) Passwords must conform with the following requirements for a "strong" password
            i. Be between 8 and 20 characters
            ii. Have at least one uppercase letter
            iii. Have at least one lowercase letter
            iv. Have at least one number or symbol").
            v. Passwords must not be easily guessable (i.e., child name, birthdate, etc).
        (ii) Users may not write their password down or save their passwords anywhere that another person could have access to.
        (iii) Users must log off and/or lock all computers and workstations if such would be unattended and accessible to a third party, even if only for a few minutes.

(c) *Protection from Malicious Software*. The Security Officer will provide education to workforce members on applications and mechanisms for safeguarding IS and PHI from malicious software including but not limited running periodic security scans and not downloading files from untrustworthy sources. Workforce members are responsible for:

(i) Reporting suspicious/unauthorized/malicious activity
(ii) Reporting suspected network, hardware or software security vulnerabilities
(iii) Reporting suspicious requests
(iv) Not opening, downloading or clicking on any links in emails from unknown senders or where the recipient is not expecting anything from the apparent sender (i.e., emails masquerading as from a known person), and forwarding any such emails to the attention of the Security Officer.

(d) *Log-in Monitoring.* The Security Officer will educate workforce members on DCG' s processes for monitoring all log-ins and log-in attempts, procedures for temporary suspending access after failed log-in attempts, and procedures required to re-activate access after failed log-in attempts. The Security Officer will implement reasonable log-in monitoring processes to monitor log-ins to all IS with PHI. In the event that a user is locked from accessing DCG Information Systems through his or her user credentials, the user should contact IS and complete a Work Order to reset his or her user credentials. Users must also immediately notify IS and the Security Officer in the event that a User suspects that the confidentiality of his or her credentials have been compromised.

(f) *Mobile Devices.* The Security Officer will ensure that workforce members are appropriately educated on the privacy and security risks associated with mobile devices and other portable media through which PHI may be created, maintained, accessed or transmitted in accordance with DCG's Transmission of EPHI and Device and Medial Controls P&S Policy. **DCG will consult as appropriate guidance made available by the Office for Civil Rights in creating training and educational materials for workforce members**
http://www.healthit.gov/DCGs-professionals/your-mobile-device-and-health-information-privacy-and-security

HIPAA SECURITY POLICIES:
ADMINISTRATIVE SAFEGUARDS

Topic: SECURITY INCIDENT PROCEDURES

Date Adopted: 3/17/2020

I. POLICY

DCG treats HIPAA Security Incidents with the highest concern and regard and will take action to identify and address any potential or actual security incidents as soon as reasonably possible. DCG will develop, implement, maintain and update these Security Incident procedures as may be reasonably necessary in order for DCG to identify and respond appropriately to Security Incidents. DCG takes such steps as reasonable and necessary to:

(1) *Detect and Identify* potential and actual Security Incidents;

(2) *Investigate* and *Evaluate* potential and actual Security Incidents;

(3) *Respond* to the Security Incidents as reasonable and appropriate;

(4) *Mitigate* any harmful effects from the Security Incidents, to the extent reasonably practicable; and

(5) *Correct and Prevent* subsequent similar or dissimilar Security Incidents.

II. PROCEDURES

1. Detection and Identification.

   (a) All employees, agents or vendors of DCG must report any potential/suspected or actual/known Security Incident to the Privacy or Security Officer as soon as possible and without delay. A Security Incident may include *attempts or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in DCG' s information systems.*

   (b) Business Associates (BAs) will be required to **report** discovery of any suspected or actual Security Incidents as soon as reasonably practicable but in any case within sixty (60) days following the actual or constructive delivery of the Security Incident by the Business Associate or its subcontractors, employees, agents, or other workforce members.

   (c) The Security Officer will periodically audit all systems containing electronic PHI for evidence of unauthorized accesses, uses and other Security Incidents, including all

locations from which electronic PHI may be accessed (e.g., computer workstations, laptops).

(d) The Security Officer will periodically evaluate all systems, policies and procedures to identify any security gaps or improper practices and procedures and take such reasonable steps as may be necessary to improve, modify or otherwise respond to such identified security gaps or practices and prevent the occurrence or re-occurrence of Security Incidents.

2. Investigation and Evaluation.

(a) The Security Officer and the Privacy Officer will investigate all reported potential and actual Security Incidents. Such Officers will investigate, gather and document all information relating to the facts and circumstances of a Security Incident. All reported incidents must be evaluated to determine whether a given Security Incident rises to the level of a Security Breach, as defined in DCG' s Security Breach Notification and Mitigation of Improper Disclosures.

(b) To the extent necessary, the Privacy and Security Officer may engage third party consultants, outside counsel and experts, including but not limited to data forensics and other experts, to assess a Security Incident.

(c) All pertinent information gathered during any Security Incident investigation must be documented, including but not limited to any determinations that a Breach did not occur or that there was no reasonable possibility of misuse.

(d) The Security Officer and/or Privacy Officer will document and retain all of the information obtained through investigation and evaluation concerning a Security Incident or Breach for a period of six (6) years.

3. Response.

(a) The Privacy and Security Officer will respond to any Security Incidents as identified by investigation and evaluation as reasonably appropriate and necessary, including but not limited to corrective and mitigative action as necessary and implementing sanctions against violating employees.

(b) The Privacy and Security Officer will respond to any Security Incidents that are reasonably believed to be a Security Breach in accordance with DCG's Security Breach Notification & Mitigation Of Improper Disclosures P&S Policy, including but not limited to providing notice of the Security Breach to affected individuals.

4. Correction, Mitigation and Prevention. The Privacy and Security Officer will take reasonably necessary steps to mitigate the harmful effects, as far as reasonably practicable of any Security Incident and/or Breach, including evaluative, disciplinary, and other corrective action as may be appropriate to decrease the risk of harm and/or prevent re-occurrence of the Security Incident

and/or Breach, and implementing additional or modifying processes and procedures as may be reasonably necessary to address identified security gaps.

HIPAA SECURITY POLICIES:

ADMINISTRATIVE SAFEGUARDS

Topic: SECURITY BREACH NOTIFICATION & MITIGATION OF IMPROPER DISCLOSURES

Date Adopted: 3/17/2020

I. POLICY

DCG strives to comply with federal and state law regarding security breach notification requirements applicable to a "Security Breach" of "Protected Health Information" (PHI) or "Personal Information" (PI) as such terms are defined under the applicable laws and these P&S Policies. Specifically, in the event of a Security Breach of PHI and/or PI, DCG follows the applicable standards of:

- The HITECH Act, and specifically §13402 (the "Breach Statute");
- HHS Final Rule for Breach Notification for Unsecured PHI (45 CFR Parts 160 and 164) (the "Breach Notification Rule"); and
- The New Jersey Identity Theft Prevention Act ("NJITPA"), and particularly N.J.S.A. 56:8-161 et seq. (the "NJITPA Breach Statute");

For purposes of this Policy, "Personal Information" or "PI" means the following under the NJITPA: an individual's **first name or first initial and last name**, linked with *any one or more of the following data elements:* (a) Social security number; (b) driver's license number or State identification number; or account number or credit/debit card number in connection with a security code, access code, or password which would permit access to such account/credit/debit number.

II. PROCEDURES

1. Detection and Internal Reporting.

   (a) DCG will implement reasonable and appropriate processes to detect potential or actual Security Breaches. Any employee, agent or other DCG vendor, including a Business Associate, who obtains information or has reason to believe that an unauthorized use or disclosure of PHI, including a Security Incident or a Security Breach, has or may have potentially occurred is required to immediately report such information to a supervisor or directly to the DCG's Privacy or Security Officer. Any complaints received will be reviewed and investigated as appropriate.

   (b) Systems will be routinely and periodically audited for evidence of Security Breaches in accordance with applicable DCG P&S Policies. The Security Officer may engage Information Technology (IT) consultants or vendors as reasonable and necessary in order to develop IT solutions for appropriate detection of security breaches within DCG's systems. The Privacy

Officer will also conduct periodic and routine auditing as required by applicable DCG P&S Policies.

(c) Business Associates (BAs) will be required to report discovery of any Security Breaches (or potential Security Breaches) as soon as reasonably practicable but in any case within **sixty (60) days** from the constructive or actual discovery of the Security Breach by the BA, BAs employees, agents or other workforce members, and BAs subcontractors. Reports from Business Associates will be forwarded to the Privacy Officer and Security Officer for documentation, review and coordination under this policy, as well as follow-up with the Business Associate as needed.

(d) Initial and periodic training of employees and other workforces will be completed as reasonably necessary in accordance with DCG's Training Policy and Procedures.

2. Investigating and Evaluating. The Privacy and Security Officer will investigate and evaluate any and all reports of unauthorized uses and disclosures of PHI, including Security Incidents and/or Breaches, and conduct a Risk Assessment within the meaning of the Security Breach Notification Laws. DCG will not retaliate or take any harassing or intimidating action against any individual who in good faith reports an unauthorized or potentially unauthorized use or disclosure of PHI, regardless of whether such results in a Security Incident or Breach.

3. Risk Assessment. **Each suspected or actual Security Incident or unauthorized use or disclosure must be treated under the presumption that the impermissible use or disclosure of PHI is a reportable Breach for purposes of HIPAA and HITECH.** If DCG determines that there is a "low probability that the PHI was compromised" as a result of the impermissible use or disclosure, DCG may conclude that a Breach did not occur requiring notice as set forth in this Policy. The Security Officer together with his or her designees shall be primarily responsible for investigating and evaluating potential Security Incidents involving ePHI, and the Privacy Officer shall be primarily responsible for investigating and evaluating other unauthorized uses and disclosures of PHI/PI to determine whether a Breach has occurred for purposes of this Policy and the Breach Notification Laws. The Privacy and Security Officers will investigate, collect, document and analyze all facts and circumstances surrounding a potential Breach using the process set forth in this Policy and the attached **Security Breach Assessment**. The Privacy and Security Officers will work together as needed to fully assess a potential Breach. **Consider and assess the following factors when conducting a Risk Assessment:**

(a) **The Nature and Extent of the PHI.** For this factor, consider the *type* of PHI involved, such as if the PHI was of a more "sensitive" nature. An example is if credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud are involved, then this would ***cut against*** finding that there is "low probability" that the PHI was compromised. With respect to clinical information, consider things like the *nature of the services*, as well as the *amount* of information and *details* involved. "Sensitive" information is not just things like STDS, mental health or substance abuse.

(b) **The Unauthorized Person who Accessed/Used the PHI.** For this factor, consider who the unauthorized recipient is or might be. For example, if the recipient person is someone at another Covered Entity or Business Associate, then this may support a finding that there is a lower probability that the PHI has been compromised since CEs and BAs are obligated

to protect the privacy and security of PHI in a similar manner as the CE or BA from where the breached PHI originated. Another example given is if PHI containing dates of health care service and diagnoses of certain employees was impermissibly disclosed to their employer, the employer may be able to determine that the information pertains to specific employees based on other information available to the employer, such as dates of absence from work. In this case, there may *be more than a low probability* that the PHI has been compromised.

(c) **Whether the PHI was actually Acquired/Viewed.** For this factor, DCG must investigate and determine if the PHI was *actually* acquired or viewed or, alternatively, if only the *opportunity existed* for the information to be acquired or viewed. One example given here is where a Covered Entity mails information to the wrong individual who opens the envelope and calls the Covered Entity to say that he/she received the information in error. In contrast, a lost or stolen laptop is recovered and a forensic analysis shows that the otherwise unencrypted PHI on the laptop was never accessed, viewed, acquired, transferred, or otherwise compromised, the Covered Entity could determine that the information was *not* *actually* acquired by an unauthorized individual even though the opportunity existed.

(d) **Mitigation.** For the fourth and final factor, DCG must consider the extent to which, and what steps need to be taken to mitigate, and once taken, how effective the mitigation was. For example, DCG may be able to obtain and rely on the assurances of an employee, affiliated entity, Business Associate, or another Covered Entity that the entity or person destroyed PHI it received in error, while such assurances from *certain* third parties may not be sufficient.

3. Breaches of PI. In most circumstances, where it is determined that there is a Breach of PHI containing electronic PI, there is also a Breach for purposes of the NJITPA. Legal should be consulted where electronic PI is affected by an incident to determine any additional state reporting obligations. Where the only PI compromised or potentially compromised is paper PI, then only HIPAA will apply, and not the NJITPA.

4. Breach Exceptions. A disclosure of PHI or PI which is encrypted in accordance with DCG's policies governing encryption, and where any decryption code, password or other mechanism is not compromised, is not a Breach. An unauthorized use or disclosure is also not a Breach where the unauthorized use or disclosure meets one of the following three exceptions. An incident must be fully evaluated as required by this Policy in order to determine whether it meets one of the below exceptions, which shall be documented on the Security Breach Risk of Harm Assessment with Breach Log.

   a. Any unintentional acquisition, access, or use of PHI or PI by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.
   b. Any inadvertent disclosure by a person who is authorized to access PHI or PI at a covered entity or business associate to another person authorized to access PHI or PI at the same

covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted by the Privacy Rule.

c. A disclosure of PHI or PI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

5. Response Procedures for Breaches. DCG will consult with legal counsel and other consultants as appropriate prior to responding to a Breach under this Section. If it has been finally determined that there has been a Security Breach of PHI or PI as set forth in this Policy, DCG will notify affected patients reasonably believed to have been affected, law enforcement, media, and federal and state agencies as may be required under the Security Breach Notification Laws and as follows.

(a) **Notify Patients:** Notify individuals by mailing a "Notice of Breach" letter to last known address. For decedents, notice to the next of kin or personal representative is sufficient. The Privacy Officer will be responsible for coordinating the form and substance of any notices to patients required by this Policy with Legal and outside counsel as appropriate. Substitute notice may be used if there is insufficient or out-of-date contact information that precludes written notification to the individual provided the substitute form of notice is reasonably calculated to reach the individual (i.e., making available notice concerning the breach on the Center's website and a toll free number for individuals to get additional information), and as permitted or required by the Breach Notification Laws. All notices to patients must be sent without unreasonable delay and in no case more than 60 days from discovery of the incident giving rise to the Breach. Notices for Breaches of PI may need to be withheld until the New Jersey Division of State Policy is notified by DCG. Any information provided to the State Police must be in accordance with DCG's Law Enforcement Requests and Required by Law Policies and Procedures.

(b) Take steps to **Mitigate** any harm as best as reasonably possible. For example, in the event of disclosure to an unauthorized third party, mitigation could include obtaining certifications of non-disclosure/destruction. The Privacy and Security Officers together with Legal and any outside consultants will be responsible for determining steps which may be required to mitigate any harm resulting or which may result from a Breach.

(c) Take **corrective actions**, which will be documented and retained by the Privacy Officer for a period of **six (6) years**. Reasonable and appropriate sanctions will be assessed against violating employees, as applicable, in accordance with DCG' s Sanctions Policy and Procedures.

(d) For Breaches of PHI ONLY:

(1) **Breaches Affecting 500 or More Patients:** If a Security Breach affects 500 or more individuals, the DCG provide the Secretary of HHS with notice of the breach ***without unreasonable delay*** and in no case later than 60 days from discovery of the breach. This notice must be submitted electronically by completing all information required on the form provided at: http://transparency.cit.nih.gov/breach/index.cfm.

(2) **Breaches Affecting *Fewer* than 500 Patients:** If a Security Breach affects less than 500 individuals, log the incident in the DCG' s Security Breach Log (maintained by the Privacy and/or Security Officer). Notification to HHS of such incidents (less than 500 individuals) will be submitted annually. A separate form must be completed for every breach that has occurred during the calendar year. All notifications of breaches occurring in a calendar year must be submitted **within 60 days** of the end of the calendar year in which the breaches occurred. Annual breach notifications must be submitted at: http://transparency.cit.nih.gov/breach/index.cfm.

(3) Notify prominent **Media**, where a Security Breach has affected or is reasonably believed to have affected more than 500 individuals within any given state or jurisdiction.

(4) Notify **Consumer Report Agencies**, where a Security Breach has affected or is reasonably believed to have affected more than 1,000 individuals.

(5) Notify **Law Enforcement**, if otherwise required by law. If a law enforcement official determines that a notification, notice, or posting required under the Breach Notification Laws would impede a criminal investigation or cause damage to national security, then the Privacy Officer or Security Officer may, in consultation with Legal, authorize delay as follows:

(a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

(b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.

DISCLAIMER THIS HIPAA BREACH RISK ASSESSMENT IS A TOOL, AND **NOT LEGAL ADVICE.** THIS TOOL SHOULD NOT BE USED TO SUBSTITUTE LEGAL ADVICE. THE DETERMINATION OF WHETHER A REPORTABLE BREACH HAS OCCURRED IS FACT-SENSITIVE AND SHOULD BE MADE WITH CARE AND THE ADVICE OF COUNSEL AS APPROPRIATE. *** * REMOVE DISCLAIMER BEFORE PRINTING THIS FORM * ***

Exhibit C
Security Breach Risk Assessment

Retain completed assessment for at least 6 years from the latter of: the date this assessment was completed OR the date on which the breach, if any, was reported to applicable regulatory authority

Date of Assessment: ___ /___ /20___

Date of Incident: On ___ /___ /20___ **OR** between ___ /___ /20___ **AND** ___ /___ /20___

Date Discovered: ___ /___ /20___

Affected Location(s):

_____

Identity of reporting BA (*if applicable)*:

_____

Date notice received from reporting BA (*if applicable)***:** _____/_____/20_____

1. **Describe *in general*** *the nature of the unauthorized use or disclosure, "Security Incident" or "Breach", including nature and type of information, individuals involved, and any mitigative action taken or which will be taken*:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

2. **How many individuals** were/ potentially are affected by the Security Incident or Breach?

   Total: _____ ☐ **≥ 500 or more Individuals** OR ☐ **≤ 499 or fewer Individuals?**

   Totals by State of Residence

   State Name: _____ ☐ ≥ 500 or more Individuals OR ☐ ≤ 499 or fewer Individuals?

   State Name: _____ ☐ ≥ 500 or more Individuals OR ☐ ≤ 499 or fewer Individuals?

   State Name: _____ ☐ ≥ 500 or more Individuals OR ☐ ≤ 499 or fewer Individuals?

   [*add additional States here as needed*]

3. Was the information actually **accessed, acquired, viewed or disclosed?** ❒ Yes ❒ No
   [*if the answer varies (i.e., in some cases was acquired, in others it has been confirmed that no access occurred) then document here*]

4. Was the information **encrypted**? ❒ Yes ❒ No
   [*if the answer varies, then document here*]

5. If encrypted, was the encryption *key or code* also acquired, accessed, or obtained?
   ❒ Yes ❒ No ❒ N/A

6. **Was the acquisition, access or use Unintentional?** ("Unintentional" access is defined as: (a) by a ***workforce*** member (e.g., employee, trainee, other person acting under *"authority"* of the CE or BA; (b) in ***good faith*** *unintentional*; (c) within the ***scope*** of their authority; **and** (d) not further used or disclosed "in a manner not permitted under the Privacy Rule." §164.402)
   a. ❒ Yes **[SAFE HARBOR = NO BREACH]**
   b. ❒ No
   c. ❒ N/A

7. **Was the disclosure Inadvertent?** ("Inadvertent" disclosure is defined as: (a) from a person otherwise authorized to access the PHI at the entity; (b) to another person authorized to access PHI at the same entity (or BA or OHCA); **and** (c) not further used/disclosed in a manner not permitted under the Privacy Rule.)
   a. ❒ Yes **[SAFE HARBOR = NO BREACH]**
   b. ❒ No
   c. ❒ N/A

8. **Will the PHI be Reasonably Retained?** ("Not Reasonably Retained" is defined as covered entity having a *"good faith belief"* that the person who received the PHI was or is not *reasonably able to retain the information*.)
   a. ❒ No **[SAFE HARBOR = NO BREACH]**
   b. ❒ Yes

[Go to STEP 9 ONLY IF Answers to #6 & #7 are "No" and the Answer to #8 is "Yes"]

9. **"Low Probability" PHI Compromised** [assign a number from 0-2]
   a. What was the Nature & Extent of the PHI? ❒ 0 ❒1 ❒ 2
      0 = *Not personal* or is *de-identified*
      1 = *Not Sensitive* **and** *Not significant amount/detailed*
      2 = *Sensitive* (Ex: SSN; mental health; STDs; genetic testing); **and/or** *Detailed*
   b. Who is the Unauthorized Person? ❒ 0 ❒ 1 ❒ 2
      0 = *Workforce at Covered Entity or BA* and **is** *cooperative*
      1 = *Identified third party* and **is** *cooperative*
      2 = *Unidentified third party* ***OR*** *Uncooperative individuals (including workforce)*

c. Was the PHI Acquired or Viewed? ❒ 0 ❒1 ❒ 2

0 = *Confirmed PHI was not viewed*
1 = *Opportunity existed, but not confirmed PHI was viewed*
2 = *Confirmed viewed or accessed*

d. Was the incident Mitigated? ❒ 0 ❒1 ❒ 2

0 = *Mitigated, with low risk of re-disclosure*
1 = *Mitigated, but risk of re-disclosure exists*
2 = *Not able to fully mitigate* because of circumstances

LOW PROBABILITY SCORE = _____

*(Note: A score of **0 is the lowest** and a score of **8 is highest**)*

10. **Taking into consideration the LOW PROBABILITY SCORE and any other important facts and circumstances surrounding the Breach, is it *likely* that the Breach would present a "*low probability*" that the PHI is or will be compromised?**

❒ YES, there is **low probability** that PHI is compromised – **NO NOTICE** required

❒ NO, there is a probability that the **PHI is COMPROMISED** – **NOTICES REQUIRED** [follow **HIPAA Breach Response** Policy]

Explain *why a* "YES" or **"NO" determination was reached, or which exception applied:**

_____

_____

_____

_____

_____

_____

_____

_____

Provide any additional detail on mitigative and corrective action taken, including retraining, disciplinary action and other steps to prevent similar incidents from occurring again:

_____

_____

_____

_____

_____

_____

_____

_____

Signature: _____

(must be completed by Privacy or Security Officer)

HIPAA SECURITY POLICIES:
ADMINISTRATIVE SAFEGUARDS

Topic: CONTINGENCY PLANS

Date Adopted: 3/17/2020

I. POLICY

DCG maintains contingency plans for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure or natural disaster) that damages systems that contain e-PHI, which includes:

(1) A "Data Backup Plan" that allows retrievable exact copies of e-PHI to be retrieved. **(*Required*)**

(2) A "Disaster Recovery Plan" that provides for a mechanism by which lost data may be restored. **(*Required*)**

(3) A "Emergency Mode Operation Plan(s)" that allows ***critical business processes*** to be continued for protection of the security of e-PHI while operating in emergency mode. **(*Required*)**

(4) Reasonable and appropriate periodic testing of contingency plans and revisions, where appropriate. (*Addressable*)

(5) Reasonable and appropriate period assessment and analysis of the relative criticality of specific applications and data in support of other contingency plan components. (*Addressable*)

II. PROCEDURES

1. Applications and Data Criticality Analysis. DCG will:

   a. Identify the activities and materials that are critical to daily business operations (e.g., EMR, billing processes).
   b. Identify the automated processes that support the critical services or operations (e.g., hardware; software; power supply; IT personnel).
   c. Determine the amount of time DCG can tolerate power outages, disruption of services and/or loss of capability.
   d. Identify practical and feasible *preventive* measures for each defined scenario that could result in loss of a critical service operation.
   e. Establish cost-effective and timely *strategies* for recovering the identified critical services, data or processes.

2. Data Backup and Disaster Recovery Plan. DCG will:

a. Develop and implement a **"Data Backup Plan"** to provide for the creation and maintenance of retrievable exact copies of all e-PHI.

b. Ensure back-up e-PHI is retrievable in accordance with the Data Backup Plan.

c. Develop and implement a "**Disaster Recovery Plan"** providing for the *restoration* of any data lost as a result of a system "interruption" (e.g., fire, vandalism, natural disaster, system failure).

3. Emergency Mode Operation Plan. DCG will:

a. Develop and document one or more Emergency Mode Operation Plan(s) (or "EMOPS") in the event of an emergency (e.g., system failure, blackout, fire, natural disaster) to enable continuation of critical business processes for protection of the security of e-PHI while operating in emergency mode.

b. An EMOP should be activated when an emergency that may impact critical business processes is reasonably anticipated, as well as during an actual emergency. The determination to activate an EMOP can be made by [*insert who*] of DCG who believes that such action will protect the security of e-PHI.

c. Make available an emergency call list to all workforce members of DCG.

d. Ensure that workforce personnel and/or individuals that must be provided access to the e-PHI of DCG in the event of an emergency or a disaster are listed in the EMOP.

e. Ensure that all appropriate agreements are in place with outside vendors key to the disaster recovery plan.

f. Train all appropriate workforce members as to their responsibilities in each EMOP.

4. Testing and Revision of Procedures. DCG will:

a. Test all procedures at least annually. If possible, outside vendors may be involved in testing exercises. If it is not "*reasonable and appropriate"* to conduct periodic testing of contingency plans and revise related procedures accordingly, **document** the reasons why and a reasonable alternative (see attached Appendix).

b. Assess the relative criticality of specific applications and data in support of other contingency plan. Consider the following: (1) network architecture diagrams and system flowcharts showing structure, equipment and system interdependencies; (2) critical business processes and their associated outage tolerance; (3) key applications and systems used to support critical business processes; (4) Other: [*list other considerations here]*

c. Maintain a list of key applications and systems and their recovery time objectives. If it is not "*reasonable and appropriate"* to conduct periodic assessment and analysis of the relative criticality of specific applications and data in support of other contingency plan components, DCG will **document** the reasons why and a reasonable alternative here:

- It is not "*reasonable and appropriate"* to implement such procedures because: (***insert description here)***

- The reasonable alternative that will be used to implement such procedures is:

(***insert description here)***

HIPAA SECURITY POLICIES:

ADMINISTRATIVE SAFEGUARDS

Topic: EMAIL/TRANSMISSION OF PHI

Date Adopted: 3/17/2020

I. POLICY

The purpose of this Policy is to set forth processes for use of e-mail and transmission of PHI at DCG, require that e-mail etiquette is followed, and educate workforce on management's right to monitor, capture, read, print, and use, any electronic mail on DCG's system.

II.PROCEDURES

A. The electronic mail system ("e-mail") maintained and operated by DCG is for the sole purpose of conducting DCG's business. All electronic communications, including any information and documents included therein, are the property of DCG.

B. DCG's management reserves the right to, and may, monitor all internal, incoming Internet, and outgoing Internet electronic communication and transactions. Management may seize and/or delete any electronic mail transaction on DCG's network. There should be no expectation of privacy when using DCG's System.

C. Each employee with a DCG-issued e-mail account (each, an "**Official E-mail Account**") are responsible for managing their e-mail accounts and ensuring their e-mail is deleted when appropriate. E-mail accounts are limited] in size per use. However, employees should understand that e-mails may be recoverable even after deletion, and that employees must never delete e-mails in an effort to obstruct or interfere with ongoing litigation or investigation, or to hide evidence or potential evidence of wrongdoing.

D. Employees are expected to use only their Official E-mail Account for conducting official business for and on behalf of DCG. Personal accounts, such as G-mail or equivalents, including personal email servers, shall not be used to conduct official work on behalf of DCG. This includes, but is not limited to a prohibition on use of "auto-rule" forwarding (i.e., automatically forwarding emails from an Official E-Mail Account to a personal account).

E. E-Mail accounts showing no activity for six months or more may be removed in DCG's discretion.

Personal Use

A. DCG allows employees "minimal" personal use of Official E-mail Accounts. Computer communications must be consistent with conventional standards of ethical and proper conduct, behavior and manners and are not to be used to create, forward or display any offensive or disruptive messages, including photographs, graphics and audio materials as judged by Management. Notwithstanding the above, there should be no expectation of privacy when using DCG's e-mail system.

B. Employees are expected to report to their any incident of perceived harassment or discrimination occurring via e-mail.

C. Employees are not to use Official E-mail Accounts as their sole personal e-mail account.

D. No DCG employee shall intentionally destroy or permanently remove from DCG documents or Electronically Stored Information (ESI), from DCG's server/email account once advised by a director or officer that the documents or ESI are related to litigation involving DCG, its employees, agents, other workforce members, Trustees or Officers.

E-Mail Use & Transmission

A. It is mandatory that employees read and maintain their Official E-mail Account in order to retain the privilege of having a personal account. E-mails should be read and addressed in a timely manner. Official E-mail Accounts should be maintained by deleting or archiving outdated or unnecessary e-mails (including those from the Deleted and Sent folders) in order to remain within the network's limit.

B. E-mails should only be sent to those individuals who are absolutely necessary in each e-mail. Use a contact list where possible to avoid sending e-mail to every employee. When sending DCG business or other information through DCG e-mail in the performance of job responsibilities, workforce members are responsible for ensuring that the correct recipient is identified. Use verified contact lists wherever possible. DCG firewalls and other safeguards will safeguard internal e-mails exchanged between workforce members, but these firewalls will not protect e-mails which are sent to an external or incorrect recipient. In the event that an e-mail containing DCG business or other information, including patient information, is sent to the wrong recipient, workforce are responsible for immediately notifying their supervisor or the Privacy Officer.

C. EMPLOYEES SHOULD NEVER CLICK ON LINKS OR OPEN DOCUMENTS FROM UNKNOWN RECIPIENTS. Even if an e-mail appears to be from someone known, do not open any documents, download any files, or click on any links that are not expected without independently verifying with the sender outside of the email communication. If a suspicious e-mail is received, immediately notify the Privacy Officer and Security Officer, and forward a copy to their attention.

D. Organization-wide emails should be limited in size to avoid overloading mail accounts. If the e-mail has attachments or embedded graphics, check the size of the e-mail prior to sending. Large e-mails will fill up other recipients' accounts unnecessarily.

E. Only use the high importance flag on critical emails where justified.

F. Do not use backgrounds or unnecessary graphics.

G. PHI concerning past, current or future patients of DCG or other information of a confidential nature should only be sent through DCG E-mail as related to the performance of job responsibilities (i) if the recipient is internal and authorized to access/use the PHI (i.e., another DCG workforce member) and (ii) if it would not be reasonable to make the PHI available to the intended recipient through an alternate mechanism. E-mails containing PHI or confidential information should never be sent to a departmental/organizational wide contact list.

H. PHI should only be sent to or received from an external recipient (i.e., a contracted provider, a patient family member) as related to the performance of job responsibilities (i) if the recipient is authorized to access/use the PHI, (ii) if it would not be reasonable to make the PHI available through an alternate mechanism and (iii) the PHI is encrypted. PHI may only be sent unencrypted if approved in advance by the Privacy Officer or Security Officer. Password protection on a document (i.e., Word) does not qualify as encryption.

I. Where sending PHI and other confidential information is authorized by this Section, the header of the email must read "CONFIDENTIAL INFORMATION" or "CONFIDENTIAL PHI". The header must never include PHI (i.e., patient name or other identifying information, health information, etc.). Each e-mail must be further accompanied by the E-Mail Confidentiality Statement. The e-mail must only contain the minimum amount of PHI necessary to accomplish the intended purpose.

J. Employees shall <u>never</u> forward an email which contains PHI to a personal email account (i.e., Gmail or equivalent). This includes personal email accounts of the employee and third parties, and irrespective of whether or not the email is encrypted.

K. Texting of PHI is prohibited except for use of a secure application or other mechanism authorized by the Security Officer or Privacy Officer. The employee will be held personally liable if there are issues resulting from non-compliance with this policy.

HIPAA SECURITY POLICIES:

TECHNICAL SAFEGUARDS

Topic: ACCESS CONTROLS

Date Adopted: 3/17/2020

I. POLICY

Only to those persons or software programs that DCG has granted rights to access in accordance with HIPAA and its P&S Policies may access PHI created, stored or handled by DCG. The following are used to accomplish the foregoing:

- Assignment of Role-Based (e.g. clinical care) & Task-Based (e.g. tech support) access to workforce members based upon job functions, licenses, experience and other factors.
- A unique user identification system by assigning a unique name and/or number for identifying and tracking identity. **(*Required*).**
- Emergency access procedures for obtaining necessary e-PHI during an emergency. (***Required***).
- "*Reasonable and appropriate"* electronic procedures that terminate an electronic session after a predetermined time of inactivity (e.g., "automatic logoff"). **(*Addressable*)**.
- "*Reasonable and appropriate"* mechanisms to encrypt and decrypt e-PHI. **(*Addressable***)

II. PROCEDURES

1. **Assessment & Evaluation.** The Security Officer will:

   (a) Identify the applications and systems that require access controls. The focus will be on the applications or systems housing e-PHI (e.g., stand-alone PC, laptops, system network).

   (b) With respect to all applications, systems and data where it has been determined that access control is required, determine the ***scope and degree*** of access control needed. (e.g., *how is the system being accessed: Is the data and/or system being accessed remotely? Is the data being viewed only? Is the data being modified? Is new date being created and stored on the system?*)

2. **Unique Identifier & Password**. The Security Officer will:

   (a) Assign a unique identifier to all systems users. For physicians, this unique identifier will be accompanied by a ***confidential personal code (CPC)*** to be used for authenticating and digitally signing or finalizing entries into electronic patient records;
   (b) Ensure that system activity can be traced to a specific user (e.g., record entries, modifications, deletions) and ensure that the necessary data is available in the system logs to support audit and other related business functions;

(c) Set password requirements and controls (e.g., requiring system users to choose password with combination of symbols, letters and numbers, with minimum password lengths).

3. **Access Controls.** The Security Officer will:

(a) Assess, develop and assign role-based and type-based access rights for all workforce members (e.g. administrative and clerical staff, RNs, PAs) in accordance with DCG's Scope of Access By Members of the Workforce P&S Policy. Such access controls should be determined based upon the nature and classification of the systems/networks being accessed and the Data maintained therein, the level of granularity available through such system/network and any identified cyber security risks, threats or vulnerabilities.

(b) Ensure workforce functions and access to systems and Data are limited and separated based on job responsibilities and the minimum necessary to perform such responsibilities.

(c) Implement "lock-out" controls after no more than six (6) failed log-in attempts or the limitation placed upon access for the system.

(d) Implement electronic procedures that terminate an electronic session after ten minutes or other appropriate time of inactivity (e.g., "automatic logoff"). If it is not "*reasonable and appropriate"* to implement automatic logoff procedures**,** the reasons why and a reasonable alternative **will be documented here:**

- It is not "*reasonable and appropriate"* to implement such procedures because:
  (insert description here)

- The reasonable alternative that will be used to implement such procedures is:
  (insert description here)

(e) Implement re-authentication controls requiring confirmation of identity and authority prior to finalization or transmission of entries.

(f) Implement automatic flagging or "tasking" where workforce member entry requires physician authentication/signature prior to entry finalization or order transmission (e.g., prescriptions for Schedule II-V controlled substances, orders for diagnostic and laboratory tests entered by RNs).

(g) Implement mechanisms to encrypt and decrypt e-PHI. If it is not "*reasonable and appropriate"* to implement mechanisms for encryption and decryption**,** the reasons why and a reasonable alternative **will be documented here:**

- It is not "*reasonable and appropriate"* to implement such procedures because:
  (insert description here)

- The reasonable alternative that will be used to implement such procedures is:
  (insert description here)

(h) Implement training mechanisms to ensure workforce members are educated on:

i. Permissible and impermissible uses and disclosures of PHI/Data;

ii. Selecting "strong passwords";

iii. Not "borrowing," sharing, writing down or posting passwords;

iv. Not modifying, entering or deleting PHI/Data while another individual is logged on or allowing another individual to modify, enter or delete PHI/Data while he or she is logged on.

4. **Access Removal.** DCG will ensure that:

(a) Users may NOT engage in any activity that is illegal under state, federal or international law while using DCG's systems. DCG will suspend or terminate Users from access to its systems *at a minimum* where:

i. The User is suspended or terminated from employment with DCG;

ii. The User is on temporary leave of absence;

iii. The User is suspected or known to have accessed or disclosed PHI/Data improperly (e.g., disclosed to a third party, accessing co-worker PHI;

iv. The User attempts to circumvent system access controls and authentication procedures or other security mechanisms;

v. Change in User's task or role.

(b) If an actual or potential "Breach" is identified by DCG, DCG will take such steps as may be reasonably necessary in accordance with DCG' s Security Incident Procedures and Security Breach Notification & Mitigation of Improper Disclosures. DCG will implement additional sanctions as may be appropriate in accordance with DCG' s Sanctions P&S Policy.

5. **Audit Controls**. DCG will develop audit controls for tracking:

(a) all system logins and failed login attempts;

(b) Identity of patient and type of PHI/Data that was accessed, entered, modified or deleted by each User;

(c) Data and time of access/entry/modification/deletion;

(d) User digital authentication and "signatures;"

6. **Emergency Access.** DCG will:

(a) Identify a method of supporting continuity of operations should the normal access procedures be disabled or unavailable due to system problems.

(b) Emergency access procedures should be activated when *necessary,* as determined by the Privacy or Security Officer, in consultation with DCG's Board.

(c) Emergency access procedures will be supported by those individuals designated by DCG to support this process.

7. **Encryption.** DCG will implement encryption as reasonable and appropriate for all PHI that is created and maintained by DCG.

(a) DCG will implement appropriate encryption mechanisms, as appropriate, for all PHI which may be maintained, accessed or created by workforce members, including but not limited to any portable or remote devices.

(b) If it is not "*reasonable and appropriate"* to implement encryption mechanisms, DCG will **document** the reasons why and a reasonable alternative here:

- It is not "*reasonable and appropriate"* to implement such procedures because: ***(insert description here)***

- The reasonable alternative that will be used to implement such procedures is: (***insert description here)***

HIPAA SECURITY POLICIES:

TECHNICAL SAFEGUARDS

Topic: AUDIT CONTROLS

Date Adopted: 3/17/2020

I. POLICY

DCG implements reasonable processes to record activities within its information systems that contain or use e-PHI through hardware, software and/or technical and procedural mechanisms and periodically examined in order for DCG to audit compliance and to detect any other unauthorized uses of e-PHI.

II. PROCEDURES

1. The Security Officer will determine how decisions on audits and reviews will be made, who is responsible for the overall audit process and results, the frequency of audits, how they will be analyzed, the sanction policy for workforce member violations and maintenance of audit information.

2. DCG will periodically and routinely conduct a Risk Assessment to identify the systems or activities that DCG will track or audit as well as current technological infrastructure, hardware and software capabilities. The focus will be on the e-PHI that is most at risk. DCG will use the results of the risk assessment to determine which systems and activities should be tracked and audited. At a minimum, DCG will monitor **Create, Read, Update, & Delete** and related system functions.

3. DCG will maintain audits logs which collectively track and monitor all information systems, user activity and Data accessed and disclosed by workforce members. Audit activity will be maintained within the defined capabilities of each system and/or application but at a minimum should include:

    (a) Date and time of login/logout or login attempt;
    (b) Identified failed logins and system lock-outs
    (c) Source/type of information system or Data which was accessed;
    (d) Identity of the user, including where applicable and available, the action which was taken;
    (e) Identity of the Individual whose Data was accessed

4. Audit logs will be immutable and reviewed at least annually. Any suspect activity or potential security incident will be reported promptly to the Security Officer. Existing system capabilities and tools for auditing will be evaluated for effectiveness and changes or upgrades made as necessary.

5. DCG will conduct routine and periodic audits to assess, monitor and evaluate information systems, compliance by workforce members, the occurrence of unauthorized accesses, and any potential or actual security incidents.

6. DCG will determine how decisions on audits and reviews will be made, who is responsible for the overall audit process and results, the frequency of audits, how they will be analyzed, the sanction policy for workforce member violations and maintenance of audit information.

7. DCG will ensure that workforce members are trained on how the review/audit policy could affect them.

8. DCG will address how the exception reports will be reviewed, where the monitoring reports will be filed and maintained, whether there is a formal process in place to address system misuse, abuse and fraudulent activity and how appropriate workforce members will be notified regarding suspect activity.

9. Audit logs will be maintained for a period of six (6) years from the date on which the PHI/Data is accessed. Risk assessments performed during an applicable EHR Incentive Program Meaningful Use Reporting Period/MACRA MIPS will be retained for a period of six (6) years following the date of attestation for that reporting period.

HIPAA SECURITY POLICIES:

TECHNICAL SAFEGUARDS

Topic: INTEGRITY

Date Adopted: 3/17/2020

I. POLICY

DCG implements processes to protect e-PHI from improper alteration or destruction through implementation of "*reasonable and appropriate"* mechanisms to corroborate that e-PHI has not been altered or destroyed in an unauthorized manner in accordance with HIPAA.

II. PROCEDURES

The Security Officer, together with his or her designees, will:

1. Identify all users who have been authorized to Access e-PHI and all approved users with the ability to alter and/or destroy data.

2. Ensure users do not share passwords and that users log-off all systems and applications, whether on workstations or through laptops;

3. Evaluate and modify, as necessary, any access rights, authorization and access permission controls, as needed;

4. Identify any possible unauthorized sources that may be able to intercept the information and modify it, including identifying scenarios that may result in modification to the e-PHI by unauthorized sources (e.g., hackers, disgruntled employees, business competitors).

5. Ensure data is being verified and routed properly, in conformance with protocol or message standards; Assess whether data quality and transmission is safeguarded, and determine as appropriate, necessary implantation schedules for encryption via IPSec, L2TP, MSChap and other appropriate mechanisms.

6. Establish a formal (written) set of integrity requirements based on the results of the analysis completed in the previous steps, including who and how may data be transmitted (e.g., BPN for laptops; IPSec for data transmission).

7. Implement on-going procedures to address these integrity requirements. Identify which methods will be used to protect the information from modification. Identify tools and techniques to be developed or procured that support the assurance of integrity.

8. Monitor processes to assess and "audit" effectiveness of integrity safeguards.

9. Reassess integrity processes continually as technology and operational environments change to determine if they need to be revised.

10. It is not "*reasonable and appropriate"* to implement electronic mechanisms to corroborate that e-PHI has not been altered or destroyed in an unauthorized, DCG will **document** the reasons why and a reasonable alternative here:

    - It is not "*reasonable and appropriate"* to implement such procedures because: ***(insert description here)***

    - The reasonable alternative that will be used to implement such procedures is: ***(insert description here)***

HIPAA SECURITY POLICIES:

TECHNICAL SAFEGUARDS

Topic: PERSON OR ENTITY AUTHENTICATION

Date Adopted: 3/17/2020

I. POLICY

DCG implements technical processes to verify the identity and authority of each person or entity seeking access to Patient Data/PHI as a technical safeguard through DCG systems to ensure only authorized individuals access Patient information. In addition, DCG will develop an authentication process to ensure only appropriate health care professionals authenticate or "finalize" entries or orders for treatments, prescriptions and diagnostic or laboratory tests in the patient's electronic health record, in accordance with state law.

II. PROCEDURES

Authentication for System Access.

(a) Identify technological methods available for authentication. Authentication is the process of establishing the validity of a transmission source or verifying an individual's authorization claim for specific access privileges to information and information systems.

(b) Evaluate authentication options available (See **National Institute of Standards and Technology (NIST) Special Publication 800-63, "Level 2" and "Level 3" Authentication Standards** http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf).

(c) Select and implement appropriate authentication methods. Consider the following options:

(1) **Multi-factor authentication** - system will require User to enter something they "know" and something they "have."

(2) **Single-factor authentication** - system will require User to enter password and identifier/username.

(d) Evaluate methods as needed, but at least annually, and update or revise as needed.

Authentication for System Entries/Transmissions.

(a) Require treating physicians to attest to their treatment relationship with the Patient prior to entering or accessing Data through DCG systems.

(b) Require all individuals entering PHI/Data into electronic patient health records to re-authenticate their credentials before digitally "signing" or otherwise finalizing an entry into the electronic health record.

(c) Require automatic "flagging" or creation of a "task" prompting the treating physician to review and authenticate entries made by Users with limited access rights, such as administrative or clerical staff.

(d) Require physicians to finalize and authenticate all orders or entries made into patient records, whether transcribed or otherwise, unless the author of such entry has independent authority to sign-off on or otherwise authorize the entry (e.g., advanced practice nurse to ender order for treatments, prescriptions or diagnostic tests). Such sign-off or finalization will make the entry immutable and must include *at a minimum:*

(1) The physician's unique and *confidential personal code (CPC),* or similar identifier for other health care professionals and Users*;*

(2) Date and time of the "signature";

(3) Automatic creation of a back-up copy of the entry;

(4) For *prescriptions, the signature must also include the prescribing practitioner's National DCG Identifier, and/or DEA number, as well as comply with future DEA regulations governing electronic prescribing of controlled substances.*

HIPAA SECURITY POLICIES:

TECHNICAL SAFEGUARDS

Topic: TRANSMISSION SECURITY & ENCRYPTION

Date Adopted: 3/17/2020

I. POLICY

DCG implements processes to protect against unauthorized access to e-PHI that is being transmitted over an electronic communication network through implementation of "*reasonable and appropriate"* security measures to ensure that electronically transmitted e-PHI is not improperly modified without deletion until disposed of. DCG will implement encryption, as reasonably practicable, on a routine basis for any and all PHI accessed or transmitted through internal and external information systems networks, including but not limited to PHI transmitted through email.

II. PROCEDURES

1. The Security Officer, together with his or her designees will:

   (c) Identify possible unauthorized sources that may be able to intercept and/or modify e-PHI. Identify scenarios that may result in modification to the e-PHI by unauthorized sources during transmission (e.g., hackers, disgruntled employees, business competitors).

   (d) Develop and implement set of requirements for how and who may transmit e-PHI, and through what devices (i.e., desktops, laptops, smartphones, IPhones and other remote or portable devices).

   (e) Implement procedures for transmitting e-PHI using hardware/software if needed and identify methods of transmission and technical controls that will be used to protect e-PHI.

   (f) Identify additional tools and mechanisms required to support the transmission security policy.

   (g) Conduct a Risk Assessment periodically to identify and resolve any security deficiencies, and any periodic testing of security systems, networks, firewalls, anti-spyware, and other applications and processes.

   (h) Implement appropriate encryption mechanisms, as appropriate, for all PHI which may be maintained, transmitted and accessed by workforce members, including but not limited to workforce access through secure and encrypted VPN connections and mobile or portable devices (i.e., laptops).

2. The Security Officer will identify, evaluate, implement, monitor and update cyber security mechanisms as necessary and appropriate to reasonably safeguard the confidentiality, integrity and availability of all IS and data from cyber security threats and vulnerabilities and minimize the impact of such threats and vulnerabilities on business operations. The Security Officer will identify all key personnel responsible for implantation of cyber security controls. The Security Officer, along with key personnel, will assess, identify and implement additional security mechanisms in the following areas:

(a) Vulnerability testing;
(b) Intrusion Detection/Prevention;
(c) Firewalls, Active Content Filtering;
(d) Virus Scanners, other Malicious Code and Unauthorized Device Tools;
(e) Cyber Intelligence gathering;
(f) Patch management;
(g) Transmission and Data-at-Rest Encryption/decryption (e.g., IPSec);
(h) Additional User Controls.

3. If it is not "*reasonable and appropriate"* to implement encryption mechanisms, DCG will **document** the reasons why and a reasonable alternative here:

- It is not "*reasonable and appropriate"* to implement such procedures because: ***(insert description here)***

- The reasonable alternative that will be used to implement such procedures is: (***insert description here)***

- The reasonable alternative that will be used to implement such procedures is: ***(insert description here)***

HIPAA SECURITY POLICIES:

PHYSICAL SAFEGUARDS

Topic: FACILITY ACCESS CONTROLS

Date Adopted: 3/17/2020

I.POLICY

DCG limits **physical access** to electronic information systems and the facility in which such systems are housed, while ensuring that properly authorized access is allowed. This is accomplished through implementing reasonable and appropriate procedure to:

(1) Maintenance Records. DCG documents repairs and modifications to the physical components of the facility that are related to security **(*Addressable*);**

(2) Facility Security Plan. DCG implements reasonable and appropriate procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft **(*Addressable*);**

(3) Access Control and Validation. DCG implements reasonable and appropriate procedures to control person's access to facility locations based on role or function, and control of access to software programs for testing and revision. **(*Addressable*);** and

(4) Contingency Operations. DCG implements reasonable and appropriate procedures that allow facility access in support of restoration of lost data under disaster recovery plan and emergency mode operations plan. **(*Addressable*).**

II. PROCEDURES

1. Conduct an Analysis of Physical Security Vulnerabilities. The Security Officer, together with his or her designees, will:

   (a) On a periodic basis, identify and conduct an analysis of existing physical security vulnerabilities and create a "facility inventory", whether separately or in connection with a risk assessment of its information systems and EHR technology (for example, consider whether nonpublic areas are locked, cameras are utilized, and workstations are protected from public viewing)

   (b) Based on the inventory, assign degrees of significance to each vulnerability identified (e.g., High, Medium, Low). Highest priority should be assigned to: (1) Data Centers, (2) Peripheral equipment locations, (3) IT staff offices, (4) Workstation locations.

2. Corrective Actions. The Security Officer will, based on the inventory and prioritization of vulnerabilities, identify the measures and activities necessary to correct any deficiencies.
   (a) All HIPAA Security Policies governing the assessment, identification and corrective measure for deficiencies will be reviewed periodically to determine whether they need revision, and maintain them for easy review.

   (b) All necessary repairs, upgrades, and/or modifications will be made to the appropriate physical areas of DCG regularly and as needed, including but not limited to visitor areas, office workspace, and restricted areas, at the direction of the Security Officer and in consultation with facility maintenance, as applicable.

   (c) All physical components that require maintenance and/or are subject to repair will be identified and maintenance logs will be kept. Examples:
      - Grounds Security (gates, alarms etc.);
      - Building Security (doors, locks, fireproofing, sprinkler systems, smoke detection)
      - Equipment and Devices used by Security Personnel (monitors, pagers);
      - Information System Security (computers, servers, back-up systems).

   (d) The facility maintenance director will maintain physical maintenance records, which will include history of changes, upgrades and other modifications for a period of six (6) years from the date of such change, upgrade or modification.

   (e) If it is not "*reasonable and appropriate"* to document repairs and modifications to the physical components of the facility which are related to security, DCG will **document** the reasons why and a reasonable alternative here:

      - It is not "*reasonable and appropriate"* to implement such procedures because: ***(insert description here)***

      - The reasonable alternative that will be used to implement such procedures is: ***(insert description here)***

   (f) Maintenance records will be documented and maintained for **six** (**6) years.**

3. Facility Security Plan and Access Control.

   (a) The Security Officer will work with the facility maintenance director to develop a "Facility Security Plan" that addresses the physical security protection of e-PHI in DCG's possession.

   (b) If it is not "*reasonable and appropriate"* to implement procedures to safeguard a particular location at the facility and or certain equipment therein from unauthorized physical access, tampering and theft, DCG will **document** the reasons why and a reasonable alternative here:

      - It is not "*reasonable and appropriate"* to implement such procedures because:

(insert description here)

- The reasonable alternative that will be used to implement such procedures is:
(insert description here)

(c) DCG will develop facility access control procedures to limit and control access to e-PHI by staff, contractors, visitors and probationary employees. Current facility access controls will be evaluated on an ongoing basis and modified or upgraded as necessary and appropriate. If it is not "*reasonable and appropriate"* to establish procedures to control and validate a person's access to facilities based on their role or function, including visitor control and control of access to software programs for testing and revision, DCG will **document** the reasons why and a reasonable alternative here:

- It is not "*reasonable and appropriate"* to implement such procedures because:
(insert description here)

- The reasonable alternative that will be used to implement such procedures is:
(insert description here)

4. Contingency Operations. The Security Officer will ensure that:

(a) The Disaster Recovery Plan and Emergency Mode Operations Plans ("EMOP") will generally control during emergency mode operations. Under emergency circumstances, authorized entry must be provided to designated emergency response personnel.

(b) Any personnel and/or individuals that must be provided access to the e-PHI in the event of an emergency or a disaster will be identified and listed in a Contingency Plan.

(c) The Security Officer, and his or her designee, will be responsible for developing the contingency plan for facility access to DCG in the event of an emergency or disaster.

(d) If it is not "*reasonable and appropriate"* to establish procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan, DCG will **document** the reasons why and a reasonable alternative here:

- It is not "*reasonable and appropriate"* to implement such procedures because:
(insert description here)

- The reasonable alternative that will be used to implement such procedures is:
(insert description here)

HIPAA SECURITY POLICIES:
PHYSICAL SAFEGUARDS

Topic: WORKSTATION USE AND WORKSTATION SECURITY

Date Adopted: 3/17/2020

I. POLICY

It is the policy of DCG that only authorized functions may be performed on DCG workstations. Workforce members are expected to understand and execute appropriately the manner in which their functions may be performed. The physical attributes of the surroundings of a specific workstation or class of workstation will be physically limited so that access to e-PHI are safeguarded. DCG implements physical safeguards are utilized for all workstations to prevent access to e-PHI by unauthorized users.

II. PROCEDURES

1. Workstation Use. The Security Officer will work with the respective departments and managers to:
   (a) Identify all workstations, authorized functions and permitted uses.
   (b) Classify workstations based on the capabilities, connections and allowable activities for each workstation used.
   (c) Identify the expected performance of each type of workstation and User.
   (d) Develop specific workstation procedures related to the proper use and performance of particular stations.
   (e) Analyze the physical surroundings for physical attributes, including a review of the risks associated with a workstation's surroundings.
   (f) Implement procedures that will prevent or preclude unauthorized access of unattended workstations, limit the ability of unauthorized persons to view sensitive information, and erase sensitive information where necessary and appropriate.
      a. All workstations and laptops will have password-protected screen savers which activate after to protect information from unauthorized viewing and to protect CRT/LCD monitors from burnt-in images. Access to workstations and laptops becomes restricted after failed log-in attempts. Passwords should not be resent on laptops once access becomes restricted.
      b. Access cards are required to enter all laboratory and office space in which workstations that may access Data are located. All visitors, including vendors and contractors, should remain accompanied by personnel while on the premises and not be left unattended in an area with workstations.
   (g) Train employees and other workforce members on the authorized uses and requirements for their respective assigned workstations.
2. Workstation Security. The Security Officer will work with the respective departments and managers to:

(a) Identify all methods of physical access to workstations, including laptops.

(b) Identify which physical safeguards are in place (for example, locked doors, screen barriers, cameras, guard, etc.) and identify any gaps in such safeguards.

i. All workstations are physically locked to ensure unauthorized personnel may not access internal peripherals such as the hard drive. The attachment of any computer peripherals such as external hard drives and zip drives must be approved by DCG prior to being attached to any computer that can access e-PHI.

ii. The use of privacy screens will be considered for workstations/personnel that may have access to certain Data, systems or applications or be in locations that are easily accessible to personnel foot traffic or visitors.

(c) Analyze the risk associated with each type of access and determine the level of threat.

(d) Add additional physical safeguards to minimize the risk to security at workstations.

(e) Relocate workstations to enhance physical security, as needed.

(f) Periodically train employees and other workforce members on workstation security.

(g) Ensure employee access is terminated appropriately upon involuntary or voluntary separation in accordance with DCG' s P&S Policies.

HIPAA SECURITY POLICIES:
PHYSICAL SAFEGUARDS

Topic: DEVICE AND MEDIA CONTROLS

Date Adopted: 3/17/2020

I. POLICY

If hardware and electronic media containing e-PHI or data may be accessed during **removal**, **movement** or **disposal** of such hardware or electronic media, then DCG implements procedures to protect such hardware and media during such period of movement. DCG will ensure that the receipt, installation and removal of all hardware, software, devices and other media that contain or through which Data is accessed or transmitted is safeguarded through:

- Comprehensive inventorying of all hardware, software, devices and media through which Data may be maintained and/or accessed;
- Procedures to address the final **disposition** of Data and the final **disposition** of the systems or hardware on which it is stored;
- Procedures for removal of Data before any device or media is made available for **reuse**;
- A reasonable and appropriate system for keeping maintenance records that document all movements of all devices and media, and the Department or person responsible therefore, including a history of all repairs, upgrades and modifications; and
- Reasonable and appropriate methods to create retrievable, exact copies of Data when reasonable and necessary before movement of any device or media.

II. PROCEDURES

1. Inventory of Devices and Media. The Security Officer will maintain a complete inventory of all hardware, software, servers, applications, devices and media through which Data may be maintained and/or accessed, locally or remotely. Such inventory should be conducted annually and periodically as necessary in response to upgrades and modifications, new acquisitions, or security incidents such as loss or theft. Removable devices and media are managed and tracked subject to the "Access Controls" P&S Policy.

2. Disposal & Reuse of e-PHI/Data. The Security Officer will:

   (a) Identify all e-PHI/Data maintained by DCG and the location(s) where such Data is maintained.

   (b) Evaluate and review the methods for disposal of e-PHI/Data for each location identified.

   (c) Consult the **NIST SP 800-88, Guidelines for Media Sanitization.** Determine and **document** the approved methods to dispose of hardware, software, and the Data itself. This will include selected processes for destroying e-PHI/Data on hard drives and file servers such as:

- C*learing* – using software or hardware products to overwrite media with non-sensitive data;
- *Purging* – degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains;
- *Destroying* – disintegrating, pulverizing, melting, incinerating or shredding.

At a minimum, disposal mechanisms will be documented for the following:

- **Hard drives.**
- **Software.**
- **Servers and data bases.**
- **Laptops**.
- **Other devices and removable media.**

(d) Ensure that e-PHI/Data is properly destroyed and cannot be recreated through specific location-specific procedures governing disposal.

(e) Implement procedures for how to **reuse** electronic media, and turn it over to IT, as appropriate.

(f) Ensure that e-PHI/Data previously stored on electronic media cannot be accessed and reused.

(g) Identify all removable devices, and review and approve all permitted uses. If certain devices cannot be removed off premises, specify which on the device.

(h) Select the individual(s) and/or department that are responsible for coordinating the disposal of data, and the reuse of the hardware and software.

(i) Train all employees and other workforce members on the security and risks to e-PHI/Data when reusing software and hardware.

3. Equipment Relocation – Accountability & Backup. The Security Officer will:

(a) Maintain records relating to hardware, media and personnel.

(b) Ensure that e-PHI/Data is not inadvertently released or shared with any unauthorized party.

(c) Maintain a record of the movements of hardware and electronic media, and the person responsible for them. ("Equipment Relocation History"). If it is not "*reasonable and appropriate"* to maintain a record of equipment relocation history and a record any person responsible for them, DCG will **document** the reasons why and a reasonable alternative (see attached Appendix).

(d) Develop and implement backup procedures to ensure that the integrity of e-PHI/Data will not be jeopardized during equipment relocation.

(e) Retain and protect an exact, retrievable copy of the data until equipment relocation is completed. If it is not "*reasonable and appropriate"* to create a retrievable, exact copy of e-PHI when needed, before movement of equipment, **document** the reasons why and a reasonable alternative.

(f) Develop and implement a *"Contingency Plan"* procedure to control in the event of failure of data backup (See DCG Contingency Plans Policy and Procedures).

HIPAA SECURITY POLICIES:

PHYSICAL SAFEGUARDS

Topic: DATA BACKUP & RECOVERY

Date Adopted: 3/17/2020

I.POLICY

DCG ensures that Data is appropriately stored, backed-up and recovered in order to maintain its accessibility for the performance of key operations and services in the event of system failure or other disaster. DCG implements reasonable and necessary administrative, physical and technical safeguards to backup Data and safeguard such backup copies of Data.

II. PROCEDURES

1. The Security Officer is responsible for overseeing the physical and online backup and recovery of Data. This will include but is not limited to overseeing and managing any reciprocal remote data hosting agreements and/or any additional online or physical data protection and recovery, as well as accesses to such copies of Data. The Security Officer together with the applicable departments and management are responsible for implementing reasonable and necessary administrative, physical and technical safeguards to protect copies of Data and provide adequately for disaster recovery in connection with the policies and procedures applicable to data backup and disaster recovery.

2. Data Storage. All Data should be stored electronically, as reasonably possible, in the appropriate system files and folders. Any Data maintained in paper format should be kept in locked containers or areas, as appropriate, and protected against unauthorized access from personnel, vendors, contractors and visitors to the DCG facility. All electronic Data is maintained for a period of ninety (90) days online in the respective system servers and is then copied to tape and maintained for an additional ninety (90) days. The Security Officer is responsible for ensuring all Data maintained on tape is appropriately disposed of in accordance with DCG' s Disposal of PHI & ePHI P&S Policy.

3. *Data Backup & Recovery. All user and system Data should be backed up regularly to ensure its availability as part of business continuity.*

    (a) Critical Data; Services. The Security Officer should work with the respective departments and management to identify user and system Data that are considered critical to DCG operations and document such Data. Such Data should be identified as critical in connection with the development and implementation of contingency policies and procedures as set forth in the DCG "*Contingency Plan*" Policy and Procedures.

(b) Automatic Backups. Backup copies of Data are currently maintained for a period of thirty (30) days online whereupon such Data is copied to tape and maintained for an additional thirty (30)] days at an offsite facility.

(c)Reciprocal Data Hosting Agreement. (if applicable) The Security Officer will be responsible for implementing and monitoring a **reciprocal data hosting agreement** with a third-party organization, as reasonable and appropriate, to facilitate the automatic backup of TIER1 Server Data. Such Data will be made available through an access portal (e.g., Citrix) in the event of system failure or other environmental disaster or emergency. The Security Officer together with the applicable departments and management will be responsible for developing policies and procedures governing the circumstances under which such Data may become available and the Departments and personnel authorized to access the Data through the Citrix portal. The Security Officer should ensure that DCG complies with any obligations under such agreement and that such agreement adequately safeguards the confidentiality, integrity and availability of PHI.

HIPAA SECURITY POLICIES:
PHYSICAL SAFEGUARDS

Topic: DISPOSAL OF PHI & E-PHI

Date Adopted: 3/17/2020

I.POLICY

DCG prohibits the disposal of PHI and e-PHI into dumpsters, recycling bins, garbage cans, trash receptacles, or in any other manner that could make it generally accessible by the public or other unauthorized persons. DCG applies appropriate administrative, physical, and technical safeguards, as required by HIPAA, in connection with disposal and destruction of all PHI and e-PHI. Workforce members and Business Associates are required and expected to ensure that PHI is maintained, disposed of and destroyed in accordance with this Disposal Policy and as required by federal and state law in order to protect the privacy of PHI and safeguard such information from potential unauthorized access and use.

II.SCOPE & APPLICABILITY:

1. This policy will apply to the following individuals and entities:

   (a) DCG, which will include its current affiliated entities and any other affiliated entities that may be created, established, or acquired after the adoption of this Policy;

   (b) All members of DCG' s Workforce (as defined below);

   (c) HIPAA Business Associates, who are not considered members of DCG' s Workforce but nevertheless access or otherwise handle DCG' s PHI pursuant to a HIPAA Business Associate Agreement in order to perform other services or functions for or on behalf of DCG and may dispose of such PHI in connection with the performance of such obligations; and

   (d) HIPAA Business Associates that are contracted by DCG for the specific purpose of disposing of PHI in accordance with this Policy and HIPAA.

2. This Policy applies to the following information:

   (a) All PHI that is or may be generated by or on behalf of the DCG, including on paper or electronic media. "Paper PHI" may include, medical charts, prescription labels, claims and billing information (e.g., EOBs), and patient logs, among other things. "Electronic PHI" may include computer hard drives, disks, memory sticks, flash drives, electronic medical records, laptops, and e-mail, among other things.

(b) All PHI created, collected, stored, handled and disposed of "**on-site**" or "**off-site**" (as defined below).

III.PROCEDURES

1. Safeguards & Disposal Methods.

(a) PHI must be safeguarded at all times from access by non-workforce members (e.g., the public) or unauthorized Workforce members, even when it is thrown out as waste or garbage or waiting to be properly destroyed.

(b) Secure containers will be provided, and secure areas will be designated where paper PHI and electronic PHI must be disposed of before it is destroyed. PHI in forms such as labeled prescription bottles or hospital identification bracelets will be maintained in opaque bags or locked containers in a secure location until they can be disposed of properly.

(c) Waste containers or designated areas that are used to temporarily hold or store PHI before it is destroyed must remain secured and/or locked. Keys or access cards to locked containers or areas where PHI is maintained should be provided only to those employees directly responsible for managing or handling destruction of the PHI. Other safeguards will be taken as reasonable and necessary to protect the privacy of PHI, such as installing surveillance cameras for monitoring.

(d) Unless the PHI is rendered indecipherable or unreadable, PHI should not be thrown out or disposed of in any manner that would make PHI potentially accessible to the *general public* or *unauthorized persons*, such as unlocked dumpsters, recycling bins or trash cans.

2. Final Disposal - Destruction of PHI.

(a) Paper PHI will be destroyed during final disposal by shredding, incinerating or otherwise rendering indecipherable the information such that it is no longer readable or identifiable.

(b) Electronic PHI will be destroyed during final disposal by clearing (using software or hardware products to overwrite media with non-sensitive data), *purging* (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or *destroying* (disintegration, pulverization, melting, incinerating, or shredding) the electronic PH such that the Data/e-PHI is rendered indecipherable, unreadable or unidentifiable. The Security Officer will ensure that Electronic PHI is disposed of in accordance with industry standards and best practices, including but not limited to NIST SP 800-88, Guidelines for Media Sanitation. No network SQL, file server, hardware, software, laptop, PDA,smartphone, flashdrive, e-mail, CD or disk will be disposed of without removing Data/e-PHI as required by this Section.

(c) Electronic PHI on electronic media must be destroyed as set forth above before such media is reused, and before "final disposal." If circumstances warrant the destruction of the electronic media prior to disposal, destruction methods may include disintegrating, pulverizing, melting, incinerating, or shredding the media.

(d) Workforce and/or Business Associates responsible for disposal of media and proper removal of electronic PHI will consult and follow NIST SP 800-88, Guidelines for Media Sanitization.

(e) When DCG contracts an *outside vendor* to handle final disposal of PHI, it will ensure that such vendor:

- Complies at all times comply with requirements under HIPAA for disposal and destruction of PHI (vendors who provide certification of compliance with HIPAA in connection with disposal of PHI are preferred);
- Signs DCG' s pre-approved HIPAA-compliant Business Associate Agreement (BAA) (if a BAA form is proposed by the vendor, then it must be approved by DCG' s legal counsel and Privacy Officer);
- Maintains a comprehensive written privacy and security compliance program as required under the Health Information Technology for Economic and Clinical Health (HITECH) Act, as amended from time to time; and
- Maintains documentation verifying final destruction of PHI (e.g., 10 containers picked up and destroyed on specific date).

3. Off-site Disposal.

(a) When any PHI is disposed of off-site, administrative, technical, and physical safeguards must be implemented and adhered to in order to reasonably protect PHI from impermissible use and or disclosure to unauthorized individuals, and against reasonably anticipated threats or hazards to the security of electronic PHI.

(b) Workforce members and/or Business Associates who use any PHI off-site, including electronic PHI, must either:

- Return all PHI to the DCG for appropriate destruction and final disposal, OR
- Ensure final disposal of PHI is in accordance with Section 2 of this Disposal Policy.

(c) All Workforce and Business Associates will follow these policies and procedures for off-site disposal of PHI, and failure to do so will result in sanctions.

4. Training & Education.

(a) DCG will ensure that all members of the Workforce PHI receive training and education on this Disposal Policy as follows:

- Training on disposal methods for PHI will be included as part of a broader annual training program, and/or provided as targeted in-service programs on an as needed basis throughout the year. Members of the workforce who do not handle PHI will also receive an appropriate level of training to ensure awareness of "appropriate" disposal methods, and allow for participation in reporting any non-compliant practices they discover;

- Attendance at training and in-service programs will be documented;

- Supplemental information will be communicated to Workforce via notices, flyers and other methods to serve as "reminders" that DCG prohibits disposal of PHI in containers and any way that could expose such PHI to access by the public and unauthorized individuals; and

- Copies of training materials, notices and training attendance sheets will be maintained for six (6) years.

(b) New members of the Workforce, including employees, volunteers etc., will, at a minimum, be given information contained in this Disposal Policy and be required to sign off that they have reviewed, understand and will follow DCG' s requirements and restrictions pertaining to disposal of PHI. New Workforce members will participate in the next available training covering DCG' s disposal practices.

5. Reporting.

(a) Each member of DCG's Workforce, and each employee of a HIPAA Business Associate that knows of conduct or circumstances that may suggest that this Policy is being violated will promptly inform the Privacy Officer.

(b) Reporting methods implemented will allow for reporting in person, by telephone, in writing, or by e-mail.

(c) The Privacy Officer will promptly evaluate and, as necessary, complete any additional investigation of the reported alleged violation of this Policy as determined to be reasonable and appropriate.

6. Monitoring Compliance.

(a) The Privacy Officer will monitor compliance with this Policy by regularly inspecting trash bins, dumpsters, and other public areas for PHI that may have been inappropriately disposed of.

(b) Verification of final disposal of PHI will be tracked and documented. The Privacy Officer will perform random audits of such documentation of final disposal. If a HIPAA Business Associate is utilized, the Business Associate will provide, upon request, documentation verifying dates and number of containers of PHI disposed.

7. Response to Violations.

(a) Each member of the Workforce is expected to take appropriate action, to the extent practicable, to prevent and/or mitigate unauthorized access to any PHI that may have been disposed in any manner other than in accordance with this Policy (e.g., remove PHI from unsecured containers, if discovered). Instances of improper disposal that are discovered and mitigated by members of the Workforce should still be reported as set forth above in Section 3 of this Policy.

(b) Each potential violation that is reported to or discovered by a Supervisor or the Privacy Officer will be taken seriously, evaluated, and if necessary, investigated thoroughly. Investigation may include having discussions with Workforce, evaluating the surrounding circumstances, and reviewing documentation, among other things.

(c) If investigation reveals non-compliance by a member of the Workforce, Human Resources, or another appropriate department, will be notified to evaluate what appropriate disciplinary action should be taken.

(d) Violations that may have or could result in a Breach of PHI will also be evaluated under DCG's P&S Policies to determine if any further action and/or notification to third parties may be required.

(e) Corrective actions will be taken in response to violations of this Disposal Policy, which may include re-evaluating whether adequate safeguards are in place, and re-training certain members of or the entire Workforce.

8. Corrective/Disciplinary Action and Sanctions.

(a) Failure to comply with this Disposal Policy will result in immediate corrective/disciplinary action against the Workforce member.

(b) Depending upon the nature and severity of the violation, appropriate sanctions will be assessed and implemented by the Privacy Officer in collaboration with Human Resources, or other appropriate department. Repeat offenses will be dealt with more severely.

(c) Sanctions under this Policy may include, but are not limited to:
- Re-training
- Verbal and/or written warning
- Suspension
- Termination

(d) Any corrective/disciplinary action taken or sanctions imposed will be documented in writing and retained for a period of six (6) years.