D&D MEDICAL GROUP, LLC
HIPAA POLICIES/PROCEDURES
MANUAL JANUARY 2019

Effective Date: October 1, 2018

Outline by Section

I. Statement of General Purpose, Applicability, Definitions

Purpose

D&D Medical Group, LLC and its subsidiaries (collectively, "D&D") recognizes that an individual's right to preserve the confidentiality of his or her health information is a fundamental legal and ethical right. These Privacy Policies and Procedures (the "Policies") reflect D&D's commitment to guard the privacy of each patient's protected health information (or "PHI") in accordance with the Health Insurance Portability and Accountability Act's Administrative Simplification provisions ("HIPAA"), The HITECH Act, and the HIPAA Regulations at 45 CFR Parts 160-164, inclusive of the "Privacy Rule" at 45 CFR Part 160 and Part 164, Subparts A and E, as amended and "The Security Rule" at 45 CFR Part 160 and Part 164, Subparts A and C, and other applicable federal and state laws governing the use and disclosure of patient information.

Definitions

Generally, terms used in these Policies should be understood to carry the same meaning as they do in HIPAA, the HIPAA Regulations and other applicable federal and state laws governing the use and disclosure of patient information. Some terms have been specifically defined here for ease of reference

PHI includes any health information, whether in electronic, paper, oral or other form that identifies, or could be used to identify an individual, whether or not the individual is currently a D&D patient. This includes, for instance, any information contained in a patient medical record, a billing record, a note taken by a receptionist about a possible, future patient, or a conversation between staff members about a prior patient.

D&D qualifies as a "healthcare provider" under HIPAA and conducts certain standard electronic transactions and thus is a HIPAA "covered entity." These Policies and Procedures include the standards and requirements with which health care providers/covered entities must comply under HIPAA and other law.

Unless otherwise noted, HIPAA and these Policies apply to the members of D&D's "Workforce," which is defined to include any employed staff or non-employed persons who are under the direct control of D&D. This will include any volunteer workers.

The role of the "Privacy Officer" is described per policy below. The Privacy Officer is Norys Rivero, who maybe contacted at (305)269 -8099 x103.

II. General Privacy Procedures and Applicability

D&D is committed to complying with HIPAA and relevant state laws as well as the following limitations on uses and disclosures of PHI. These Policies provide general guidance that reflects the more specific guidance provided in later applicable policies.

1. PHI shall not be used or disclosed except as otherwise permitted or required by HIPAA, other law, or these Policies.

2. PHI may be disclosed to the individual who is the subject of the PHI, or to the individual's "personal representative."

3. PHI may be used or disclosed to carry out Treatment, Payment or Health Care Operations ("TPO").

4. PHI may be used or disclosed as "incident to" (i.e., as a by-product of) a use or disclosure otherwise permitted or required under these policies if the use or disclosure is:

    a. Done in accordance with the "minimum necessary" requirements; and

    b. Made under "reasonable care" to limit such incidental uses or disclosures.

5. Any other use or disclosure of PHI requires a valid Authorization, unless otherwise permitted or required under these Policies or applicable law.

6. For any use or disclosure, other than for Treatment purposes or those made to the individual or as required by law, D&D shall use or disclose only the "minimum necessary" amount of PHI in order to accomplish the purpose of the use or disclosure.

7. "De-identified" information, i.e., information that does not or could not be used to identify an individual, should be used to avoid unnecessary disclosure of information consistent with "minimum necessary" rules.

8. If necessary for research, public health and Health Care Operations only, D&D should use a "limited data set," i.e. patient information with specific identifying information redacted.

9. In the event that PHI is used for research purposes, these Policies will be amended to provide for same.

10. D&D will not sell PHI.

11. D&D will not use PHI for fundraising or marketing purposes without a written Authorization.

12. These policies and procedures apply to living patients and continue to apply for fifty (50) years following a patient's death.

III. D&D 's Commitment to Ensuring Privacy and Security of PHI

a. Designation of a Privacy Officer

Purpose:
D&D is committed to ensuring the privacy and security of PHI. To effectively coordinate, manage, and implement activities related to those efforts, D&D appoints a Privacy Officer. This policy will describe the Privacy Officer position. Questions regarding this policy, or its application to a particular factual situation, should be directed to the Privacy Officer.

Policy:
The Chief Executive Officer will appoint D&D's Privacy Officer for a renewable annual term. The Privacy Officer will be responsible for the development, revisions and implementation of D&D's HIPAA, and other related, policies and procedures. The Privacy Officer will also be responsible for receiving complaints and reporting complaints and outcomes to senior management. The Privacy Officer has the authority to review all documents

and other information within D&D relative to privacy and security activities, including, but not limited to, encounter forms, billing information, claims information, patient medical records, contracts, and other clinical and financial information.

Procedure:

1. The Privacy Officer will be trained on all policies and procedures necessary to fulfill his or her responsibilities in ensuring the security and privacy of PHI.

2. The Privacy Officer will oversee and monitor the development and implementation of the policies and procedures contained herein, and will oversee disciplinary actions for non-compliant individuals.

3. The Privacy Officer will facilitate regular educational programs relating to the D&D's privacy and security policies and procedures.

4. The Privacy Officer will facilitate reviews relating to the privacy and security policies and procedures set forth herein, including audits and gap analyses.

5. The Privacy Officer will review and monitor performance of vendor contracts and Business Associate Agreements with respect to privacy and security matters.

6. The Privacy Officer must ensure that processes are implemented to maintain compliance with Federal and state laws, and is responsible for periodically revising the policies in light of changes in the needs of D&D or changes in the law.

7. The Privacy Officer with the assistance of counsel, will independently investigate and act on complaints or breaches of the HIPAA security and privacy policies and procedures policies.

8. The Privacy Officer will service as a resource to D&D's designated liaison to regulatory and accrediting bodies for matters relating to HIPAA privacy.

9. The Privacy Officer must coordinate with senior management and the Compliance Officer, Human Resources, and D&D's counsel in carrying out his or her responsibilities.

10. The Privacy Officer will report to the Chief Executive Officer

b. Workforce Training Regarding the Use and Disclosure of Protected Health Information

Purpose:

D&D is committed to ensuring the privacy and security of patient health information. Federal, state, and/or local laws and regulations have established standards with which health care organizations must comply when using or disclosing an individual's PHI. To support our commitment to patient confidentiality, all employees and other members of the D&D workforce will receive appropriate training regarding the policies and procedures for using and/or disclosing PHI, as required under 45 C.F.R. §164.530(b) and other applicable federal, state, and/or local laws and regulations. Questions regarding this policy, or its application to a particular factual situation, should be directed to the Privacy Officer.

Policy:

1. D&D will train all employees and other D&D Workforce members, as applicable, regarding the proper use and disclosure of PHI.

2. Training will occur within a reasonable time of initial employment or engagement, and be repeated thereafter at least annually.

3. In addition, training will be provided to each member of the Workforce whose functions are affected by a material change in these policies or procedures, within a reasonable period of time after the material change becomes effective.

Procedures:

1. Training regarding the use and disclosure of PHI will include the following, without limitation:

    a. The process by which an individual may request the use or disclosure of his or her PHI;
    b. The process by which D&D may request the use or disclosure of an individual's PHI;
    c. The documents to be used for individuals to request that their PHI be used or disclosed for specific purposes;
    d. The process by which D&D may solicit a request from an individual to use or disclose his or her PHI for D&D's own use;
    e. The documents to be used for D&D to solicit a request for an individual's PHI to be used or disclosed by others;
    £ The right of the individual to revoke an Authorization;
    g. The identification of defective Authorizations;
    h. The recognition of when D&D may condition the provision to an individual of Treatment, Payment, enrollment, or eligibility for benefits on the provision of obtaining an Authorization; and
    i. The process for investigating and anal ing potential breaches.

2. Training will be conducted by, or under the supervision of, the Privacy Officer.

3. The Privacy Officer will maintain records of all training.

c. Safeguarding PHI

Purpose:

HIPAA requires that Covered Entities take appropriate administrative, technical, and physical steps to safeguard PHI. Many of these steps will be taken through polices governing the operation of D&D computer networks, filing systems, and the physical security of D&D premises as required under the HIPAA Security Rule. This policy will provide procedures for Workforce members to follow with regard to PHI that is, unavoidably, in use and therefore potentially exposed to other patients or Workforce members who have no job duties related to the PHI.

Policy:

There shall be appropriate safeguards to protect the privacy of PHI. Workforce members must, at all times, take reasonable precautions to shield PHI from casual observers, other patients, or other unauthorized personnel. The below procedures provide examples of typical situations where PHI may be inadvertently exposed to view, but Workforce members should not limit their efforts to the specific situations described below. Questions regarding this policy, or its application to a particular factual situation should be directed to your supervisor or the Privacy Officer.

Procedure:

1. Workforce members shall make all reasonable efforts to limit incidental uses or disclosures of PHI when making a use or disclosure that otherwise is permitted or required under these policies and procedures. Examples include the following:

    a. When discussing PHI all conversations should be held at as low a volume as is reasonably possible. Workforce members should exercise professional judgment in determining if highly sensitive conversations should be held in more private settings, if reasonably possible.
    b. When stepping away from exposed PHI, whether in electronic or hard copy form, personnel should take effort to cover PHI and overall remove the PHI from plain sight.
    c. To the extent applicable, hard copy patient records, when not in use by Workforce members, shall be maintained in a secure area. Essential information may be kept on hand during the provision of services, but that information shall be maintained in a chart that has a cover. Electronic patient records should be not be left unattended on screens which are visible to others.
    d. Sign-in sheets shall ask for only the minimum necessary information. This may include items such as the patient's name and appointment time. Sign-in sheets shall not ask for diagnosis or Treatment-related information. Sheets should be periodically removed from the clipboard and stored in a secured fashion.
    e. Passwords to computer programs shall not be written on post-it notes in plain view.

2. Workforce members who believe that PHI is not being properly safeguarded or that it has been released without Authorization should immediately contact the Privacy Officer.

d. Sanctions for Violation of D&D 's Privacy Policies and Procedures

Purpose:

HIPAA requires that Covered Entities such as D&D provide for appropriate sanctions for Workforce members who violate required policies or procedures. This policy will describe how sanctions will be determined and applied.

Policy:

D&D shall apply appropriate sanctions against members of its Workforce who fail to comply with these policies and procedures.

Except as set forth below, the Privacy Officer, in consultation with D&D 's counsel, Human Resources and/or the Compliance Officer shall determine the appropriate sanction in the case of a violation of these policies and procedures, to ensure that sanctions are consistent with the Human Resources policies and requirements. Sanctions may vary depending on factors such as the severity of the violation, whether the violation was intentional or unintentional, or whether the violation indicated a pattern of improper use or disclosure of PHI, and may range from a verbal warning to a written warning to suspension to termination.

Procedure:

1. The Privacy Officer will determine what sanctions are appropriate with input, as required, by D&D 's counsel, Human Sources, Compliance Officer, executive team and/or Board of Directors.

2. D&D may apply stronger sanctions (such as termination) without first using milder sanctions (such as a warning), if the violation is very severe in the professional judgment of those in authority who are involved and who review the matter, or if there is a pattern of multiple violations and if consistent with D&D 's employment policies.

3. If it is determined that the Privacy Officer must be sanctioned, D&D 's Chief Executive Officer in consultation with D&D 's counsel, shall determine and impose the sanction based on the criteria set forth above.

4. D&D shall document all applied sanctions, and shall retain this documentation for ten (10) years from the date of its creation or the date on which it was last in effect, whichever is later.

5. D&D shall not apply sanctions in an effort to intimidate or retaliate against a member of its Workforce who engages in protected activity related to a good faith reporting related to suspected unlawful activities described in these policies, or who reports PHI as a crime victim.

e. Prohibiting Retaliation Against Employees; Individuals, or Others

Purpose:

D&D will take all necessary steps to refrain from intimidating, threatening, coercing, discriminating against, or taking any other retaliatory action against any employee, individual, or other for the exercise of any right under, or for participation in any process established applicable laws and/or regulations. Questions regarding this policy, or its application to a particular factual situation, should be directed to the Privacy Officer.

Policy:

1. It is the responsibility of all D&D employees to report perceived misconduct, including actual or potential violations of laws, regulations, policies, procedures of D&D relating to the privacy and security of PHI of patients.

2. D&D will maintain an "open-door policy" at all levels of management to encourage employees to report problems and concerns.

3. D&D will follow all necessary procedures to protect against any retaliation toward any employee, individual, or other for exercising their rights or participating in any process pursuant to internal policies, applicable law, and/or regulation.

4. Any employee who commits or condones any form of retaliation will be subject to discipline up to, and including, termination.

Procedures:

1. D&D will not retaliate against employees, individuals, or others for:

    a. exercising any right under, or participating in any process established by federal, state, or local, law, regulations, or policy;

b. filing a complaint with D&D and/or with a federal or state agency;
c. testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing;
d. Opposing in good faith any act or practice made unlawful by federal, state, or local law, regulation, or policy, provided that the manner of the opposition is reasonable and does not itself violate law.

IV. Documentation and Record Retention

Purpose:

HIPAA requires that Covered Entities such as D&D maintain written documentation of their compliance with HIPAA's requirements. This policy will provide the policy and procedures governing HIPAA record retention and documentation.

Policy:

Whenever written communication, documentation, or record is required by these policies and procedures or applicable law, D&D shall maintain the written communication or an electronic copy of it according to the procedures outlined below. Questions regarding documentation or record retention should be directed to the Privacy Officer.

Procedure:

1. The Privacy Officer shall be responsible for maintaining the records described in this policy and ensuring their retention, security, and privacy as appropriate.

2. Whenever written communication is required by these policies and procedures or applicable law, D&D shall maintain the written communication or an electronic copy.

3. Whenever documentation of an action, activity or designation is required, D&D shall maintain a written or electronic record of the action, activity or designation.

4. Unless otherwise expressly provided otherwise, all documentation required in these policies and procedures shall be maintained for at least ten (10) years from date of its creation or the date when it was last in effect, whichever is later, unless a longer retention period is required by another D&D policy.

5. For patients who were under the age of 18 years old at the time of treatment, documentation shall be maintained for at least (10) years following their 18th birthday.

6. The following is a non-inclusive summary list of documents required to be maintained. In case of any doubt, the decision to retain or destroy documentation should be referred to the Privacy Officer.

   a. These policies and procedures, and any revised versions thereof
   b. Authorizations for the use or disclosure of PHI.
   c. Revocations of Authorization for the use or disclosure of PHI.
   d. The Notice of Privacy Practices and any revisions thereof
   e. Each patient's written acknowledgment of his or her receipt of the Notice of Privacy Practices.
   f All Business Associate Agreements and Sub-Business Associate Agreements.
   g. All restrictions that D&D agrees to with respect to its use or disclosure of a patient's PHI, including restrictions created at the request of a patient after that patient has paid out-of-pocket for Treatment, and any termination of those restrictions.
   h. Designated Record Sets that are subject to access by the patient (i.e., medical and billing records).
   i. The information that D&D is required to provide in an accounting of disclosures (i.e., an accounting log).
   j. Any communications accepting or denying a patient or enrollee's request to amend his or her PHI in a Designated Record Set.
   k. Any accounting of disclosures of PHI provided to a patient.
   l. The titles of the persons or offices responsible for processing patients' requests to access, amend and account for their PHI that D&D maintains in Designated Record Sets.
   m. The identification of the Privacy Officer.
   n. When training was provided to each Workforce member.
   o. Any complaints received, and their disposition.
   p. Any sanctions that are applied to a member of the Workforce.
   q. Any documents related to inadvertent loss, access, disclosure, or inappropriate uses of PHI (breach documentation).
   r. Any other document or type of document or group of documents identified for retention by the Privacy or Compliance Officer.

V. Individual's Rights Regarding PHI

a. Notice of Privacy Practices

Purpose

HIPAA requires that all patients receive a copy of D&D's "Notice of Privacy Practices" (the "Notice" - a plainly worded document that describes how D&D uses and discloses PHI and each patient's rights with regard to their own PHn. This Policy document will describe how Notices will be provided to patients and how the provision of notices will be documented.

Policy

Each patient shall receive a copy of D&D's Notice, as updated from time to time by D&D's Privacy Officer or D&D's counsel. No Workforce member shall use or disclose PHI in a manner inconsistent with the notice currently in effect. The notice must be approved by Privacy Officer, or D&D's counsel.to ensure that it meets the requirements of HIPAA. Questions regarding this policy, or its application to a particular factual situation, should be directed to the Privacy Officer.

Procedures

1. The Privacy Officer shall promptly revise and distribute the Notice whenever there is a material change in a privacy practice as described in the Notice or when there is a change to applicable law that requires changes to the Notice (where, for instances, the HIPAA regulations providing required Notice content are changed). Changes requiring a revision of the Notice could include, without limitation, changes to:

    a. How PHI is used or disclosed,
    b. The patient's rights regarding their own PHI,
    c. D&D's legal duties, or

d. Any other changes, internal or external to D&D operations, which affect how D&D handles PHI and that are appropriate for the Notice.

2. Revisions to the Notice shall not be implemented prior to the effective date of the revised Notice, except as required by law.

3. Revised Notices must be posted and provided to new patients. Revised Notices need not be sent to patients who already received a Notice, but they should be available upon request to existing patients.

4. Each patient shall receive a copy of the Notice no later than the date of first service delivery, including services delivered electronically or, in an emergency treatment situation, as soon as reasonably practicable.

5. Responsible Workforce members shall make a good faith effort to obtain written acknowledgment from each patient of his or her receipt of the Notice according to the acknowledgement form attached to the Notice (e.g., front desk personnel).

6. In an emergency, D&D may attempt to obtain the written acknowledgement after the emergency is resolved.

7. If written acknowledgement cannot be obtained, the responsible Workforce member shall document the good faith effort to obtain written acknowledgment and the reason why it was not obtained.

8. D&D shall keep copies of the Notice available at its offices to distribute to individuals who request a copy, and shall post the Notice in a clear and prominent location where patients seeking services can reasonably read the Notice. The Notice will be posted in a prominent location on D&D website, and made available electronically. D&D may provide the Notice by e-mail to individuals who agree to an electronic Notice.

9. A copy of each version of the Notice shall be retained for ten (10) years from the date of its creation or the date it is last used, whichever is later. A copy of each signed acknowledgement, or a description of D&D's good faith efforts to obtain such written acknowledgement, shall be retained for ten (10) years from the time the acknowledgement was obtained or sought, or was last in effect, whichever is later.

b. Individual's Right to Request Restrictions on Uses and Disclosures

Purpose:

HIPAA provides patients with the right to request a restriction on the use and disclosure of their PHI for certain purposes, and with certain limitations. D&D is required to accept and consider these requests, though it is not required to agree to a requested restriction, except in the case of a patient's explicit request that PHI related to a service paid entirely out-of-pocket by the patient not be disclosed to a payer for Payment or Health Care Operations of D&D, unless such disclosure is required by law. This policy will provide for procedures regarding handling and responding to requests for such limitations.

Policy:

Each D&D patient has the right to request a restriction on the use and disclosure of his or her PHI for the following purposes:

- To carry out Treatment, Payment, or Health Care Operations.
- To a family member, friend or other person involved in the individual's health care.

The Privacy Officer or D&D's counsel will receive and determine appropriate responses to all such requests according to the procedures described in this policy. Questions regarding this policy, or its application to a particular factual situation, should be directed to the Privacy Officer or Cano's counsel.

Procedure:

1. All requests for a restriction on the use or disclosure of their PHI should be forwarded or directed to the Privacy Officer.
   D&D is not required to agree to a requested restriction, except as stated above with respect to a service entirely paid for out-of-pocket by the patient.

2. If D&D agrees to a restriction, the Privacy Officer or Workforce member shall document such agreement in a form and manner approved by the Privacy Officer.

3. If D&D agrees to a restriction, it is binding and D&D may not use or disclose PHI contrary to such documented agreement except if the patient is in need of emergency treatment and the restricted PHI is needed for such treatment by D&D or another health care provider.

4. If restricted PHI is disclosed to another health care provider as allowed for emergency treatment, D&D shall request that the other provider not make further use or disclosure of the information.

5. A patient may not request a restriction to a use or disclosure of PHI:

   a. Related to the Secretary of HHS activities to investigate or determine D&D's compliance with HIPAA, or
   b. For a purpose for which no patient permission is required.

6. D&D may terminate an agreement to restrict PHI disclosures if:

   a. The patient agrees to or requests the termination of such agreement in writing.
   b. The patient orally agrees to the termination and the oral agreement is documented.
   c. D&D informs the patient that it is terminating the Restriction Agreement without the patient's agreement, except that such termination is only effective with respect to PHI created or received after the patient has been so informed.

7. D&D shall retain documentation of each restriction agreement for ten years from the date it was created or was last in effect, whichever is later.

c. Requests for Confidential Communications

Purpose:

HIPAA provides patients with the right to request to receive communications from their healthcare providers through alternate means or at alternate locations in order to preserve confidentiality of the information being communicated. This policy will provide the procedures D&D will follow in receiving and responding to such requests.

Policy:

Consistent with state law, D&D recognizes an individual's right to request that any communication involving PHI from D&D be delivered in a confidential manner. D&D's counsel and /or Privacy Officer will receive and determine D&D 's response to such requests in accordance with all applicable laws. Workforce members should direct requests or questions with regard to this policy to D&D 's counsel and/or the Privacy Officer.

Procedure:

1. D&D shall accommodate reasonable requests in writing by a patient to receive communications of PHI by alternative means or at alternative locations.

2. The Privacy Officer will receive all such requests and respond to them in accordance with D&D policy and applicable law.

3. Workforce members who receive a request should direct the requesting patient (or forward the request itself) to the Privacy Officer for review and response.

4. D&D shall condition reasonable accommodation on receiving:

    a. Information on how payment will be handled, when applicable and appropriate; and
    b. Specification of an alternative address or other method of contact.

5. No explanation of the basis for the request as a condition of making reasonable accommodations shall be required.

d. Individual's Request to Access Their Own PHI

Purpose:

A patient may, in general, have access to their own PHI when it is maintained by a Covered Entity such as D&D in a Designated Record Set (defined in more detail below). This policy further defines the information maintained in a Designated Record Set and provide procedures by which patients may request access to this information and by how D&D employees may respond to proper requests.

Policy:

D&D patients may request access and/or a copy of his or her own PHI held by D&D for as long as the PHI is maintained in the Designated Record Set. Patients may not have access to PHI compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding.

The Designated Record Set includes the medical and billing records, including any item, collection or group of information that contains PHI, in any form (other than oral), maintained by D&D, or for D&D by a third- party. Questions regarding this policy, or its application to a particular factual situation, should be directed to the Privacy Officer.

Procedure:

Patient's Request for Access.

a. The patient's request for access to or a copy of his or her records must be made in writing. A Request for Access form may be obtained from the Privacy Officer or may be found on the D&D website or patient portal 9when operational).

   Patient Request for Access forms should be delivered to the Privacy Officer or to a location directed by the Privacy officer for action in the conformance with these policies.

b. D&D may agree to or deny the request in accordance with these procedures.

c. D&D shall act on a request for access to PHI within 30 days of receiving the request, whether by providing access or by informing the individual in writing of the denial.

2. Grant of Access.

   a. If D&D agrees to provide access and/or a copy, it shall provide for inspection and/or a copy in the form or format requested by the patient, if it is readily producible in such a format, including a machine-readable electronic format for records stored electronically. For instance, if a patient requests his or her records on a CD in PDF format, and the records are stored electronically and readily available or readily convertible to such a format, D&D shall provide the records in the requested format. If it is not readily producible, D&D shall provide access in a readable hard copy form or other such form or format (including an electronic format) as agreed upon by the individual and D&D.

   b. In lieu of providing access to the PHI, D&D may provide the patient with a summary of the requested PHI, or with an explanation of the PHI, if:

      i. The patient agrees in advance to such a summary or explanation; and
      ii. The patient agrees in advance to any fees imposed, if any, by D&D for such a summary or explanation.

   c. If the requested PHI is contained in duplicate form in more than one designated record set maintained by or for D&D, D&D need only produce the PHI once.

   d. D&D shall provide access in the time frame specified in 1. c. above.

3. If the individual chooses, it may direct D&D to transmit the copy directly to an entity or person designated by the individual, provided that any such choice is clear, conspicuous, and specific.

4. Fees. If the patient requests a copy of the PHI, or agrees to a summary or explanation, D&D my impose a reasonable, cost-based fee that includes only:

   a. A per page copying fee.

   b. Postage, if the individual requests that the information be mailed.

   c. For electronic health record copies, D&D may charge for the cost of any provided media (such as USB drives or CDs).

5. Requested PHI Not Maintained by D&D. If D&D does not maintain the requested PHI and knows where it is maintained, it shall inform the patient where to direct his or her request for access.

6. Documentation of Individual Access. The Designated Record Sets that are subject to access and the titles of persons or offices responsible for receiving and processing requests for access are maintained by the Privacy Officer. This information shall be retained for ten (10) years from the date of its creation or the date it was last in effect, whichever was later.

e. Individual's Request for Amendment of P m

Purpose:

HIPAA provides patients the general right to amend their PHI, within certain limits, and requires that Covered Entities facilitate and record amendments as appropriate. D&D will comply with this requirement. This policy will provide the procedures by which D&D will accept, review, and act on amendment requests.

Policy:

D&D will offer each patient the means to request amendments to his or her PHI. D&D will accept a patient's request to amend his or her PHI or a record for as long as the information is maintained in the Designated Record Set. Whether a record is amended as the patient requests will be determined by the Privacy Officer in conformance with applicable law and D&D policies. Questions regarding this policy should be directed to the Privacy Officer.

Procedure:

1. The Privacy Officer is responsible for receiving and processing a request for amendment. To the extent the Privacy Officer delegates this duty, such delegation shall be documented and maintained in accordance with D&D 's document retention policies.

2. A patient who requests an amendment of PHI must complete the Request for Amendment form, available from the Privacy Officer, including a reason to support the requested amendment.

3. D&D shall inform the patient in advance of requiring the patient to complete the Request for Amendment form and provide a reason for the amendment.

4. D&D shall act on a request for amendment no later than sixty (60) days after the receipt of the Request.

5. The allowed time may be extended for responding to the request by no more than thirty (30) days if:

    a. D&D is unable to take action within the allowed time frame; and
    b. D&D, within the allowed time frame, provides a written statement of the reasons for the delay and the date by which we will act on the request.

6. If D&D accepts the requested amendment, in whole or in part, it must add the amended information to the record. The original information shall not be replaced or deleted.

7. If D&D accepts the requested amendment, it shall inform the patient that the amendment has been accepted and obtain the patient's identification of an agreement to have D&D notify the relevant persons with whom the amendment needs to be shared.

8. D&D shall make reasonable efforts to inform and provide the amendment within a reasonable time to:

    a. Persons identified by the patient as having received the PHI and needing the amendment; and
    b. Persons, including Business Associates, who D&D knows have the PHI that has been amended and that may have relied on, or could conceivably rely on, such information to the detriment of the patient.

9. If D&D is informed by another provider, health plan or clearinghouse of an amendment to the patient's PHI in D&D 's Designated Record Set, it shall so amend the PHI.

10. D&D will allow patient amendments that have been properly submitted except if D&D determines that the PHI or record:

    a. Was not created by D&D, unless the patient provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment.
    b. Is not part of the Designated Record Set.
    c. Would not be available for access under D&D 's policy governing an individual's access to their own PHI.
    d. The PHI or record is accurate and complete.

11. If D&D denies the patient's request for amendment it shall provide to the patient a timely, written denial that is approved by the Privacy Officer and that is in plain language and contains:

    a. The basis for the denial;
    b. A statement that the patient may submit a written statement disagreeing with the denial, including a description of how the patient may file such a statement;
    c. A statement that, if the patient does not submit a statement of disagreement, the patient may request that D&D include the request for amendment and the denial with any future disclosure of the PHI that is the subject of the requested amendment;
    d. A description of how the patient may complain to D&D, including the name (or title) and telephone number of the contact person or office designated to receive complaints; and
    e. A description of how the patient may complain to the Secretary of HHS, which includes the name of the health care provider, the plan or clearinghouse, and a description of alleged acts or omissions, to be sent in writing within 180 days.

12. If D&D denies a Request for Amendment, it shall accept the patient's written statement of disagreement, if submitted, including the basis for the disagreement, provided however, that:

    a. D&D may reasonably limit the length of a statement of disagreement; and
    b. D&D may prepare a written rebuttal to the patient's statement of disagreement, and shall provide a copy to the individual who submitted the statement of disagreement.
    c. D&D shall, as appropriate, identify the record or PHI in the designated record set that is the subject of the disputed amendment and shall append or otherwise link the patient's request for an amendment,

the D&D's denial of the request, the patient statement of disagreement, if any, and D&D 's rebuttal, if any.

13. If a patient submitted a statement of disagreement, D&D shall include the material appended as described above, or an accurate summary of such information, with any subsequent disclosure of the PHI to which the disagreement relates.

14. If the patient did not submit a written statement of disagreement, D&D shall include the patient's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the disputed PHI only if the patient has requested such an action.

15. If D&D makes a subsequent disclosure of the disputed PHI using a standard HIPAA electronic transaction that does not permit the additional material to be included, D&D may separately transmit the required material to the recipient of the standard transaction.

16. D&D shall amend any PHI regarding a patient in the Designated Records Set maintained by or for D&D.

f. Individual's Request for Accounting of Disclosures of PHI

Purpose:

HIPAA provides patients the right to receive an "accounting," or a list of all disclosures of their PHI, within the six year period prior to the request. This right does not extend to all disclosures - certain types of disclosures need not be included in an accounting. Currently, disclosures for Treatment, Payment and Operations are not subject to the accounting, but may be, in the future, by regulation. This policy will detail the types of disclosures which need not be accounted for and will provide the procedures D&D Workforce members will follow to accept and act on patients' requests for accountings. To the extent, any applicable law or regulation change to require the inclusion of disclosures for Treatment, Payment and Operations in an "accounting," this Policy will apply to such.

Policy:

D&D recognizes that a patient has the right to receive an accounting of disclosures of PHI made by D&D in the six 6) years prior to the date on which the accounting is requested, except for disclosures that are specifically exempted. Requests for accounting will be approved by the Privacy Officer. All patient requests for an accounting should be forwarded to the Privacy Officer, who will respond in accordance with these procedures. Individuals with questions regarding their right to an accounting (or Workforce members with questions regarding this policy) should direct them to the Privacy Officer.

Procedure:

1. Patients who wish to request an accounting should provide a written request for the accounting of such disclosure to D&D at its headquarters location to the attention of the Privacy Officer. The Privacy Officer will respond to all such requests. A form of such request will be downloadable from the D&D website (or patient portal when operational).

2. D&D shall respond to a request for an accounting no later than sixty (60) days following receipt of a request.

3. If D&D is unable to comply with the request within sixty (60) days, it may extend the time for providing the accounting by thirty (30) days provided that D&D provides the patient with a written statement of the reasons for the delay and the date by which the accounting will be provided.

4. D&D shall provide the first accounting to a patient in any 12-month period without charge. D&D may impose a reasonable, cost-based fee for each subsequent accounting within the 12-month period, provided that D&D:

    a. Informs the patient in advance of the fee; and,
    b. Provides the patient with an opportunity to withdraw or modify the request in order to avoid or reduce the fee.

5. An accounting will identify all disclosures of PHI made by D&D in the past six (6) years with the exceptions of disclosures:

    a. For Treatment, Payment or Health Care Operations, until law or regulation otherwise requires the inclusion of such disclosures.
    b. To the individual or personal representative.
    c. Incident to a use or disclosure permitted under these Policies.
    d. Pursuant to an Authorization
    a. To family members, friends or persons involved in the patient's care or for disaster relief purposes.
    f For national security or intelligence purposes.
    g. To correctional institutions or law enforcement officials.

6. An accounting shall comply with the following:

    a. The accounting must include disclosures to or by a Business Associate.
    b. The brief statement of the purpose of the disclosure must reasonably inform the individual of the basis of the disclosure
    c. If the disclosure is to the Secretary of HHS as part of a HIPAA investigation or compliance review or for a purpose that does not require patient permission, D&D may attach a copy of the written request for disclosure.
    d. If D&D has made multiple disclosures to the same person or entity in response to the individual's written Authorization or a valid written request, the accounting may provide:

        i. The information required for the first such disclosure during the accounting period.
        ii. The frequency, periodicity, or number of disclosures made during the accounting period; and
        iii. The date of the last disclosure during the accounting period.

7. D&D shall document the information required to be included in an accounting, each written accounting provided to a patient, and the titles of the persons or officers responsible for receiving and processing requests for accounting, and shall retain such documentation for not less than six (6) years from the date of its creation or the date it was last in effect, whichever is later.

8. D&D shall temporarily suspend a patient's right to an accounting of disclosures to a health oversight agency or to a law enforcement official under these conditions:

    a. The agency or official submits a statement that such an accounting would be reasonably likely to impede agency's activity and specifies the time for which such suspension is required. If the statement is oral rather than written, D&D shall:

i. Document the statement and the identity of the official making the statement
ii. Temporarily suspend the patient's right to an accounting of disclosure subject to the statement; and
iii. Limit the temporary suspension to no more than thirty (30) days from the date of the oral statement unless a written statement is submitted during that time.

VI. Transmission of PHI

a. Transmission of PHI Via Facsimile

Purpose:

HIPAA permits the transmission of PHI by facsimile (fax) so long as the transmission is performed in a manner that takes into account appropriate safeguards designed to ensure the security and privacy of the PHI being transmitted. This policy, along with D&D policies regarding the confirmation of identities and otherwise maintaining the security and privacy of PHI, will provide procedures for transmitting PHI via fax.

Policy:

Workforce members should take all reasonable precautions when transmitting PHI by fax. Facsimiles are inherently insecure, subject to intercept, and prone to accidental misdirection. Occasionally, however, transmission of PHI via fax is a necessity as no other, more secure means (such as encrypted email, or direct transmission through a shared electronic health record (EHR) system or protocol) is available. As is reasonably practical, the following procedures should be followed in the course of transmitting PHI via facsimile. Questions regarding this policy, or its application to a particular factual situation should be directed to the Privacy Officer.

Procedure:

1. If available, Workforce members should use other, and more, secure modes of transmission, prior to transmitting PHI by facsimile.

2. Sensitive PHI shall not be faxed except in circumstances constituting a medical emergency.

    a. Sensitive PHI includes, but is not necessarily limited to, information concerning mental health, gender identity, drug or alcohol dependence, sexually transmitted diseases and HIV. The Privacy Officer should be consulted with regard to transmission of sensitive PHI.

3. A standard fax coversheet will be developed by the Privacy Officer for use with all facsimile transmissions. It shall be used for every transmission that includes PHI and shall be filled in completely prior to a transmission. The standard fax coversheet shall include:

    a. The following heading, in bold type: **"Confidential Health Information Enclosed."**
    b. The following statement:
    "IMPORTANT WARNING: This message is intended for the use of the person or entity to which it is addressed and may contain information that is confidential or privileged, the disclosure of which is governed by applicable law. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this information is strictly prohibited. If you have received this message by error, please notify us immediately and destroy the related message."
    c. Spaces that allow for the insertion of the following information:
        1) The sender's name, address, telephone number, and fax number;
        2) The recipient's name and fax number;
        3) The date and time of the fax;
        4) The number of pages transmitted; and

5) Information regarding the expected verification of receipt of the fax, if verification is requested.

4. A fax of PHI may request verification of receipt of the information by the proper recipient. More sensitive or urgent transmissions should request a return phone call, e-mail, page, or substantive return fax.

5. Except in emergency situations, the following faxing procedures shall be followed:

   a. The sender of a fax containing PHI shall confirm the recipient's proper fax number.
   b. If PHI is :frequently faxed to a person or organization, that recipient's fax number shall be programmed into the designated fax machine to prevent typographical errors.
   c. The confirmation fax shall be stapled or otherwise attached to the document that was faxed and included in the medical record. The disclosure via fax shall be documented as a disclosure, in the same manner as all other PHI, for the purposes of accounting of disclosures to the patient.

6. Upon learning that a fax containing PHI has been mis-routed:

   a. The sender of the fax shall contact the unintended recipient and request either the return or destruction of the document.
   b. All practical steps shall be taken to remedy the problem that caused the misdirection.
   c. The sender shall immediately provide written notice to the Privacy Officer that a mis-routing has occurred.
   d. Each of these steps shall be documented in writing by the sender of the fax and the documented record of the incident shall be promptly provided to the Privacy Officer.

7. Faxes that contain PHI and are received by employees, volunteers, medical staff members, or other individuals allowed to access PHI shall be shredded once the recipient is fmished using them for their intended purpose. This requirement does not apply when the transmitted information is to be maintained in the patient's medical record or another appropriate, secure area.

b. Transmission of PHI Via Telephone

Purpose:

HIPAA permits the transmission of PHI by telephone so long as the transmission is performed in a manner that takes into account appropriate safeguards designed to ensure the security and privacy of the PHI being transmitted. This policy, along with D&D policies regarding the confirmation of identities and otherwise maintaining the security and privacy of PHI, will provide procedures for transmitting PHI via telephone.

Policy:

Workforce members should always take all reasonable steps to conduct telephone conversations involving PHI in a manner and location that reasonably protects the privacy and security of the PHI. As is reasonably practical, the following procedures should be followed in the course of transmitting PHI via the telephone. Questions regarding this policy, or its application to a particular factual situation, should be directed to your supervisor or the Privacy Officer.

Procedure:

1. Communications involving PHI via telephones should be conducted away from main thoroughfares and gathering areas, when possible. As reasonably practical, Workforce members should transmit PHI over the phone in areas where the chance of being overheard by persons not designated to receive that information is minimized as reasonably possible.

2. Any voicemail system will be password protected to prevent unauthorized access to voicemail messages containing PHI. Any breach of this security feature shall be immediately reported to the Privacy Officer.

3. Unauthorized individuals shall not be granted access to telephones that are utilized for the purpose of receiving patient calls.

4. Patient-contact telephone numbers shall not be programmed into phones.

5. Written and computerized directories of patient-contact information will be restricted to authorized individuals only.

6. Computerized directories of patient information shall not remain displayed on a computer screen while not in use. Written directories shall not be left open, in plain sight of unauthorized individuals, while not in use.

7. Calls shall be conducted in a manner that preserves patient privacy to the greatest extent possible. Care should be taken to limit the volume of one's voice when transmitting PHI, especially if unauthorized individuals are nearby or the information is of a sensitive nature.

8. PHI may be released over the telephone in the same manner that it may be released in person, in accordance with these policies and procedures.

9. Callers should be asked to confirm their identify and provide verification as D&D Workforce members deems reasonable. This includes callers asserting to be patients representatives, law enforcement officials or even the patient.

10. Messages left for patients with the person who answers the phone or on an answering shall be limited to the following:

    a. The name of the person for whom the message is being left;
    b. A request that the patient return the call.
    c. The name of the person placing the call, but only if doing so will not reveal the clinical condition of the patient;
    d. The name of the individual whom the patient may ask for when returning the call, if applicable; and
    e. The telephone number where the call may be returned.

c. Personal Electronic Devices

Purpose:

D&D understands that personal electronic devices ("PEDs"), including "smartphones," iPADs, tablet computers, and similar small, portable, and multi-task capable electronics have become common in everyday life for many of our Workforce members. In the work environment of D&D , however, such devices make the risk of improper storage and transmission of PHI significantly greater. Since these are personal devices, they are more difficult for D&D to monitor. **Accordingly, each Workforce member who brings a PED to the workplace is personally responsible for ensuring that it is not used in a way that violates D&D 's HIPAA Policies.** This Policy and its associated Procedures will provide guidelines intended to minimize the potential for portable electronic devices being used to improperly capture, store, or transmit PHI.

Policy:

1. Workforce members should never record PHI onto personally owned PEDs without the express permission of a manager or the Privacy Officer.

2. Cameras and other recording devices should never be used in an area containing PHI. Even the accidental inclusion of PHI (in, for instance, the background of a photo) could be considered an inappropriate use or disclosure of PHI and should always be avoided.

3. Workforce members should not communicate on any PED, whether by voice, text (SMS messaging) chat, or video conference in a way that might compromise PHI. Voice functions, for instance, should be reserved to private areas where verbal PHI cannot be overheard and video chats or conferences should never take place in an area where the other party might be able to view PHI.

4. Lost or stolen PEDs containing PHI should be **IMMEDIATELY** reported to the Privacy Officer.

5. PHI should never be transmitted via a PED (other than through properly private telephone calls) unless absolutely no other options are available and the health or safety of a patient depends on the immediate transmission of the information. The Privacy Officer should be informed (after the fact, if necessary in an emergency) whenever a PED has been used to transmit PHI.

Procedures:

1. Workforce members will apply the above described Policies at all times while a PED is in their possession and they are working with or in the presence of PHI.

2. Any failure to follow the above Policies should be immediately reported to the Privacy Officer.

VII. Procedure for When PHI is Requested

a. Verification Requirements

Purpose:

HIPAA requires that Covered Entities such as D&D take reasonable steps to verify the identity of a person or persons who are requesting PHI where that identity is not already known to the person receiving the request. This policy will explain how D&D Workforce members should verify identity and how records of the verification process should be maintained.

Policy:

Prior to any disclosure of PHI except disclosures to a family member, friend or other person involved in the individual's care or for disaster relief purposes, the identity of the person requesting the PHI and the authority of any such person to access that information shall be verified by the Workforce member if that person's identity is not already known. Questions regarding the necessity or sufficiency of verification documents should be directed to the Privacy Officer or D&D's counsel.

Procedure:

1. Prior to any disclosure of PHI, any documentation, statements or representations (oral or written) from the person requesting the PHI, as required by these Policies, shall be obtained by the Privacy Officer, and such documentation, statements or representations may be relied upon by D&D as such reliance is reasonable under the circumstances.
   Example: Where a Workforce member receives a phone call requesting a patient's PHI from an unknown number and the caller represents himself or herself as representing another health care practitioner (for instance, the patient's out of state physician) the Workforce member should look up the published number for that practitioner and call that number to verify the caller's identity before providing the PHI.

2. A Workforce member may rely, if reasonable under the circumstances, on any of the following to verify the identity when disclosing PHI to a public official or to a person acting on behalf of the public official:

   a. Presentation of an agency identification badge or other credentials;
   b. A written request using the appropriate government letterhead; or
   c. Any document that establishes that the person is acting on behalf of a government official, such as a contract for services, memorandum of understanding, or purchase order, so long as the document is reviewed for sufficiency by the Privacy Officer and/or D&D 's counsel.

3. A Workforce member may rely, if reasonable under the circumstances, on any of the following to verify authority when disclosing PHI to a public official or a person acting in behalf of the public official:

   a. A written statement of the legal authority under which the information is requested on the letterhead of the public official.
   b. If a written statement would be impracticable, an oral statement of the legal authority under which the information is requested, with the approval of the Privacy Officer or D&D's counsel..
   c. A legal warrant, subpoena, order, or other legal process issued by a grand jury, court, or administrative tribunal.

4. Verification requirements are met if D&D relies on the exercise of professional judgment when using or disclosing PHI to a family member, friend, or other person involved in the individual's care, or to a disaster relief agency or to avoid a serious threat to health or safety.

Example: When disclosing PHI to an individual involved in the patient's care, such as an independent nursing aide known to the D&D Workforce member, the Workforce member does not need to confirm the aide's identity, but must seek the patient's agreement, either verbal or in writing, prior to disclosing the PHI as required by D&D policy regarding disclosures made to individuals involved in a patient's care. The agreement should be noted on the patient's record.

b. Minimum Necessary Uses and Disclosures of P m

Purpose:

Under many circumstances, HIPAA requires that Covered Entities disclose only the PHI that is reasonably necessary to accomplish the purpose of the disclosure - the "minimum necessary" PHI. This policy addresses the "minimum necessary" concept, identifies circumstances when disclosures should not be so limited, and provide procedures for identifying and disclosing only the minimum necessary PHI to sources within and outside D&D.

Policy:

When using, disclosing or accessing PHI, Workforce members shall adhere to the "minimum necessary standard and limit the use or disclosure to the minimum necessary to accomplish the intended purpose, unless the purpose is exempted from this policy, as identified below. Questions regarding the scope of this policy, or its application to a particular situation, should be directed to the Privacy Officer.

Procedure:

1. The "minimum necessary" standard does not apply to:

    a. Uses and disclosures made (or requested) for Treatment purposes. (See the Policy regarding "Treatment, Payment and Healthcare Operations" disclosures).
    b. Uses requested by or disclosures to the individual who is the subject of the PHI.
    c. Uses or disclosures made pursuant to a valid Authorization.
    d. Disclosures to the Secretary of HHS for HIPAA compliance purposes.
    e. Uses and disclosures that are required by law.

Most uses of PHI in the routine course of D&D's business will be covered by one of the above items.

2. Only those Workforce members who need access to specific PHI to carry out their duties are allowed such access. Workforce members should consult their manager or supervisor if they are uncertain whether they are permitted to access specific PHI. The Privacy Officer shall have final approval of those persons with access to PHI.

3. Workforce members shall limit any appropriate disclosures of or requests for PHI, made on a routine basis to the reasonably necessary amount of PHI necessary to achieve the purpose of such disclosure or request. For such disclosures or requests made on a non-routine basis, Workforce members shall notify the Privacy Officer who shall determine the amount reasonably necessary for the purpose of the intended disclosure or request.

4. Assuming that a specific disclosure of PHI is otherwise permitted under these Policies, a Workforce member may rely on a request for disclosure as being the minimum necessary when the information is requested by:

a. An authorized public official, if the official represents, verbally or in writing, that the PHI is the minimum necessary for the stated purposes, and the disclosure is one for which no patient permission is necessary, as listed in these Policies.
b. Another healthcare provider, health plan, or health care clearinghouse.
c. A professional who is also a member of the Workforce or is a Business Associate, if that professional represents that the requested information is the minimum necessary for the stated purpose(s).

5. No one shall use, disclose or request an entire medical record, except when the entire record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request.

VIII. Disclosures of PHI

1. Permitted Disclosures

a. **Personal Representatives (Deceased Individuals, Adults, Minors)**

Purpose

HIPAA provides certain rights to an individual's personal representative. A "personal representative" is someone who has legal authority to make decisions concerning another person's PHI. The personal representative has all of the rights of the individual under these Policies except as may be limited by the personal representative's legal authority or in situations of abuse, neglect, or endangerment (as described below).

Policy

Legal documentation such as an "Advance Directive," allows a designated individual to make decisions for a patient about their health care, in the event that the patient is, or has become, incapable of deciding for him/herself or incapable of communicating such decisions. An Advance Directive generally takes effect when the patient's doctor certifies in writing that the patient is not capable of making decisions about his/her care. A similar legal document is a "Health Care Power Of Attorney." In the absence of an Advance Directive or a Health Care Power of Attorney, the patient's relative may have authority under state law to make health care decisions on behalf of the patient. A copy of any legal document should be placed in the patient's chart. Advance Directives and Health Care Powers of Attorney may expire on the death of the patient. In the case of questions, contact the Privacy Officer for clarification of a third party's authority to act for a patient as to health care decisions.

Procedure

1. If an individual who is the subject of PHI is an adult or an emancipated minor, and another person has legal authority to make decisions for the individual (such as a legal guardian, conservator, or someone acting under power of attorney), D&D's Workforce will treat that other person as the individual's "personal representative."

2. If a parent, guardian, or other person acting in loco parentis has authority under applicable law to act on behalf of an un-emancipated minor in making health care decisions, D&D shall respect the decisions of such person as the minor's personal representative, except:

    a. The parent, guardian or other person shall not be treated as the minor's personal representative with respect to PHI if state law is contrary to this provision.

3. If an individual who is the subject of PHI is deceased, and another person has legal authority to act on behalf of the deceased individual or the individual's estate (such as an executor or estate administrator), the Workforce will treat the other person as the deceased's "personal representative."

4. A person's authority to act on behalf of a deceased individual or a deceased individual's estate is evidenced by a court document, such as "Letters of Administration." Generally, such authority is limited to matters related to the administration of the deceased patient's estate.

5. A copy of any documentation showing an individual's authority to act as a personal representative should be placed in the patient's chart. In the case of questions, contact the Privacy Officer for clarification of a document presented as a person's authority to act for a patient or, in the case of a deceased patient, the patient's estate.

6. It is the policy of D&D at its sole discretion to elect not to treat a person as the personal representative of an individual if:

    a. Based on a review of the circumstances by the Privacy Officer that there is a reasonable belief that the individual has been, or may be, subjected to abuse, neglect or domestic violence by the person seeking

to be treated as the personal representative, or treating the person as the personal representative could endanger the individual; and

b. A decision is made by the Privacy Officer, based on professional judgment, that it is not in the best interest of the individual to treat the person as the individual's personal representative.

b. Disclosure to Report Wrongful Activity

Purpose:

HIPAA permits Workforce members to use and disclose PHI where they are doing so in good faith in order to identify unlawful conduct on the part of a covered entity. HIPAA prohibits covered entities like D&D from taking retaliatory action against those reporting such unlawful activity, even where the use or disclosure of PHI may otherwise be considered an actionable violation of D&D 's policies. This policy will confirm the situations in which D&D will consider a use or disclosure to have been made in this type of unlawful activity reporting capacity.

Policy:

A Workforce member or Business Associate, as defined in these Policies, will not be sanctioned for the disclosure of PHI if he or she believes in good faith that D&D has engaged in conduct that is unlawful or that violates professional or clinical standards, or that the care, services, or working conditions provided by D&D may endanger one or more patients, workers, or the public. Questions regarding this policy, or its application to a particular factual situation, should be directed to the Privacy Officer.

Procedure:

1. Workforce members who believe in good faith that D&D or a Workforce member is acting in an illegal or inappropriate fashion should contact their supervisor, the Privacy Officer, or the Compliance Officer.

2. Workforce members with concerns regarding D&D compliance processes should consult D&D 's compliance policies or make contact with D&D 's Compliance Officer in person, through email, or by following D&D 's reporting procedures set forth in its Compliance Program.

3. A Workforce member or Business Associate will not be sanctioned for the use or disclosure of PHI if he or she believes in good faith that D&D has engaged in conduct that is unlawful or that violates professional or clinical standards, or that the care, services or working conditions provided by D&D may endanger one or more patients, workers or public as long as the disclosure is:

    a. To a health oversight agency or public health authority authorized by law to investigate or oversee D&D's professional activities;
    b. To an appropriate health care accreditation organization for the purpose of reporting the allegation of misconduct or failure to meet professional standard; or
    c. To an attorney retained by or on behalf of the Workforce member or Business Associate for the purpose of determining his or her legal options with regard to the alleged misconduct or potentially dangerous care, services or conditions.

4. A Workforce member who is the victim of a criminal act will not be sanctioned for using or disclosing PHI to a law enforcement official if:

a. The disclosed PHI concerns a suspected perpetrator of the criminal act, and
b. The disclosure complies with D&D's policy regarding uses and disclosures of PHI for which no patient Authorization is required.

c. Business Associates

Purpose:

HIPAA provides that Covered Entities may disclose PHI to "Business Associates" which are non-Workforce individuals or entities that perform a business or support function for or on behalf of D&D, and the function involves access to, use, creation, or disclosure of PHI (such as a billing company, or an IT support company). HIPAA requires that Business Associate relationships be governed by a written agreement known as a Business Associate agreement, or "BAA." This policy will provide D&D's policy and procedures for contracting with Business Associates.

Policy:

D&D maintains arrangements with various Business Associates who perform business or support functions for or on behalf of D&D involving PHI. D&D will obtain satisfactory assurances from its Business Associates that they will appropriately safeguard PHI through written contracts which comply with the requirements for Business Associate agreements set forth under the HIPAA regulations and the procedures below. Only the Privacy Officer or his/her designee may approve Business Associate relationships, and all questions related to this policy should be directed to the Privacy Officer.

Procedure:

1. The Privacy Officer shall maintain a form Business Associate agreement that, at a minimum, complies with these procedures and all applicable law.

2. The BAA form will be updated periodically, by the Privacy Officer or his/her designee as required by changes in applicable law or D&D policy.

3. The Privacy Officer must approve all changes made to the BAA form.

d. Uses and Disclosures to Carry Out Treatment, Payment or Health Care Operations

Purpose

HIPAA permits the disclosure of PHI without an Authorization where the PHI is being disclosed to carry out Treatment, Payment, or Health Care Operations, as defined under HIPAA. This Policy sets forth the HIPAA definition of those terms and provide examples of such disclosures where a patient Authorization is not required.

"Treatment" means the provision, coordination or management of health care and related services by D&D, including the coordination or management of health care; consultation with another provider relating to a patient; or the referral of a patient for health care to another provider.

"Payment" means activities undertaken by D&D to obtain reimbursement for the provision of health care, including 1) determinations of eligibility and coverage; 2) billing, claims management, collection activities and related data processing; 3) review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care or justification of charges; 4) utilization review, including pre-certification and pre-authorization for services and retrospective review of services; and 5) disclosure of certain allowed information to consumer reporting agencies in order to collect reimbursement (name, address, date of birth, social security number, payment history, account number, and name and address of the covered entity).

"Operations" means 1) quality assessment or improvement activities; population-based activities related to improving health or reducing health care costs; protocol development; case management and care coordination contacting health care providers and patients with information about treatment alternatives; certain patient safety activities, and other non-treatment-related activities; 2) reviewing the competence or qualifications of health care professionals; evaluating practitioner, provider or 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; training of non-health care professionals; accreditation, certification, licensing, or credentialing activities; 3) conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection and compliance programs; 4) business planning and development; 5) business management and general administrative activities, including privacy compliance, customer service activities, resolution of internal grievances, activities related to the sale, transfer, merger or consolidation of D&D ; and 6) the use of PHI in order to create De-identified information, creating a limited data set, or for fundraising on behalf of D&D .

Policy

Workforce members may use and disclose PHI to carry out Treatment, Payment or Health Care Operations without obtaining an Authorization as long as the use or disclosure complies with these Policies and applicable laws.
Workforce members with questions regarding this Policy should speak with the Privacy Officer.

Procedure

Workforce members may use and disclose PHI for D&D 's Treatment, Payment, or Health Care Operations purposes, as defmed by this policy. If you have a question as to whether a particular use or disclosure is for one of these purposes, you should speak to the Privacy Officer before using or disclosing the PHI.

e. Use or Disclosure of P m to Person Involved in Individual's Care

Purpose:

HIPAA permits the disclosure of PHI to a patient's family member, other relative, close personal friend, or any other person identified by the patient, when the PHI is directly relevant to that person's involvement with the patient's care or Payment for that care, provided that certain efforts are made to either obtain the patient's consent or to review the situation and determine if the disclosure is in the patient's best interest. This policy will establish procedure for such inquiries and disclosures at D&D.

Policy:

Workforce members may disclose PHI to a patient's family member, other relative, close personal friend, or any other person identified by the patient, when the PHI is directly relevant to that person's involvement with the patient's care or Payment for that care, so long as all procedures are followed to either 1) obtain the patient's consent, or 2) determine that the patient is unable to consent, and that the disclosure is in the best interest of the patient. Questions regarding this policy, or its application to a particular factual situation, should be directed to the Privacy Officer.

Procedure:

1. Workforce members may notify (or may assist in the notification of) a family member, other relative, personal representative or other person involved in the patient's care of the patient's general condition or location, provided that:

    a. If the patient is present and has the capacity to make health care decisions, the patient is informed in advance of the disclosure and (1) agrees to the disclosure; (2) is given the opportunity to verbally agree, prohibit, or restrict the disclosure and does not express a verbal objection; or (3) Workforce member(s) reasonably infer from the circumstances, based on professional judgment, that the patient does not object to the disclosure.
    Example: A wife accompanies a husband to an appointment, and follows him into the Treatment room. Workforce members could reasonably infer that the husband had no objection to the disclosure of PHI to the wife related to his Treatment.

    b. If the patient is not present, incapacitated or in an emergency, the use or disclosure should only be made where the Workforce member has determined that the disclosure is both: A) in the best interest of the patient, and B) is directly relevant to the person's involvement in the patient's care. Example: A husband stops by the office to pick up copies of exercises for a specific condition or injury for his wife, who is a patient of D&D. Staff could reasonably infer that the wife has no objection to the disclosure of PHI, in the form of the prescription, to the husband.

2. If the use or disclosure is for disaster relief efforts, (e.g. hurricane) and is to a public or private entity authorized by law to assist in such efforts, Workforce members should contact the Privacy Officer. Generally, in such situations, Workforce members will follow (a) and (b) above except if the Privacy Officer determines that these requirements interfere with its ability to respond to the emergency circumstances, in which case Privacy Officer will dictate the appropriate response based on the exercise of professional judgment.

3. Workforce members should seek guidance from the Privacy Officer before disclosing any information regarding a deceased patient to any individual other than the deceased patient's personal representative. Certain information may be disclosed, but only on the authority of the Privacy Officer.

f. Disclosures to Government Agencies and Law Enforcement.

Purpose

In addition to uses and disclosures for Treatment, Payment or Operations, HIPAA permits certain disclosures without patient Authorization, verbal agreement or any other patient permission. This Policy will describe the uses and disclosures that fall in this category and provide guidance and examples.

Policy

Workforce members must become familiar with each of the categories of uses and disclosures listed below. Prior to engaging in a use or disclosure that falls within one of these categories, Workforce members must notify and seek guidance from D&D 's Privacy Officer or counsel.

The Privacy Officer and counsel will oversee or direct any use or disclosure of PHI that falls within one of these categories to ensure compliance with these Policies and Procedures and the law. Any questions related to the application of the following circumstances should be directed to the Privacy Officer.

Procedure

PHI may be used or disclosed without patient permission to the following entities and/or under certain conditions if the use or disclosure is related to certain circumstances, including without limitation, those listed below. In these circumstances, there may be notice requirements to the patients and other requirements not set forth in the policy.

1. Required by law.

2. For public health activities

3. To an appropriate government authority and related to a report of abuse, neglect or domestic violence (other than child abuse and neglect, which would fall under public health activities)

4. To a health oversight agency for oversight activities (audits, investigations, etc.)

5. For judicial or administrative proceedings and/or in response to proper legal process, provided all related requirements are met including D&D's receipt of assurances that the patient has been notified of the request. Prior to responding to such request, D&D Workforce should bring all judicial or administrative requests or other legal process to the attention of the Privacy Officer.

6. To a law enforcement official for law enforcement purposes under certain circumstances:

    a. To make reports required by law (i.e., wounds and other injuries).

    b. To comply with a court order, a court ordered warrant, subpoena or summons, or a grand jury subpoena, provided the law enforcement official ensures they have written procedures to protect the confidentiality of records.

    c. To comply with an administrative subpoena, administrative summons, civil or authorized investigative or similar process authorized by law.

For the purpose of identifying or locating a suspect, fugitive, material witness, or missing person; however, Workforce members should contact Privacy Officer prior to disclosing any information. Privacy Officer should request investigative demand and/or subpoena before disclosing. In the absence of such documentation, the Privacy Officer should consult with D&D counsel before disclosing.

d. D&D may not disclose information related to an individual's DNA; DNA analysis; or typing, samples, or analysis of body fluids or tissue for the purposes of identification or location unless required by law or in compliance with legal process as discussed herein.

e. To a law enforcement official's request when the individual is, or is suspected to be, a victim of a crime if a) the individual agrees to the disclosure or b) D&D is unable to obtain the patient's agreement due to incapacity or other emergency circumstances, and certain circumstances are present.

£ The law enforcement officer's request may be in writing or oral, and may be in the form of a wanted poster or media report.

g. D&D may disclose PHI about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the person's death if D&D suspects the death may have resulted from criminal conduct.

h. To a law enforcement official PHI that D&D believes in good faith constitutes evidence of criminal conduct that occurred on the premises of D&D.

7. To avert a serious threat to health or safety if in "good faith," D&D believes that, under the circumstances, a use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.

8. For military and veteran activities, national security and related activities, protective services to the President and other dignitaries, and to a correctional institution or law enforcement official regarding PHI of an inmate or other individual under certain circumstances.

9. For worker's compensation purposes pursuant to the applicable laws governing workers' compensation or other similar programs to provide benefits for work-related injuries or illness without regard to fault.

1. Authorization Required

Purpose

Except under specific circumstances, such as to carry out Treatment, Payment or Operations, HIPAA requires that D&D Workforce members give the individual an opportunity to agree or object to the use or disclosure or obtain a written Authorization for any use or disclosure of PHI from the individual who is the subject of the PHI.

Policy D&D Workforce members will always, before disclosing any PHI for any purpose, determine whether an Authorization is required. Where an Authorization is required, Workforce members will use the Authorization form provided by the Privacy Officer according to the Procedures detailed below, and will appropriately maintain a copy of the executed Authorization in the subject individual's medical record. Workforce members with questions regarding this Policy or its implementing procedures should contact the Privacy Officer.

Procedure

1. An opportunity for the individual who is the subject of the PHI to agree or object is appropriate only in cases where the PHI is being disclosed to a person involved in the patient's care, such as a family member or close friend, or for D&D's patient directory. For more information, see D&D's policy regarding "Uses or Disclosures of PHI to Persons Involved in an Individual's care."

2. When an Authorization is required, Workforce members must use the HIPAA compliant and valid Authorization, approved for use by the Privacy Officer, which contains all elements required by the HIPAA. Such form will be maintained by the Privacy Officer

3. Authorizations may not be combined with any other document, except for an Authorization obtained as a condition of participating in medical research that includes Treatment (see below).

4. D&D will not condition Treatment to an individual on the provision of an Authorization for release of PHI to a third-party, except when the sole purpose of the Treatment is to obtain PHI for disclosure to the third-party.

   Example: An individual that visits a D&D therapist in order to obtain Treatment documentation from the therapist for his employer related to his condition must sign an Authorization permitting D&D to disclose the PHI to the employer.

5. An individual may revoke an Authorization at any time by so indicating in writing. No particular revocation form is required, but the revocation should be specific. The revocation shall not affect any action taken by D&D in reliance on the Authorization prior to the revocation.

6. Any signed Authorization must be retained in the patient's file pursuant to the Policy and Procedure on retention below.

   Marketing is defined to mean communication about a product or service that encourages recipients to purchase or use the product or service. D&D shall obtain a written Authorization for all marketing from the individual subject to the marketing exception where the marketing:

   a. Occurs as part of a face-to-face communication by a Workforce member to the individual; or

   b. Consists of a promotional gift of nominal value provided by D&D.

   There are certain other exceptions to the Authorization requirement for marketing communications. However, such determination as to whether a communication amounts to "marketing" for which an Authorization is

required under HIPAA shall be made (and documented) by the Privacy Officer. Whenever a communication is being made to a patient that is encouraging the recipient to purchase or use a product or service, the Privacy Officer should be consulted.

2. Use and Disclosure of De-Identified and Re-Identified Information and Limited Data Sets

Purpose:

HIPAA provides for the use of "De-identified" data and Limited Data Sets" for certain purposes. Since this data has had important identifying information removed, it may be used and disclosed certain in circumstances when PHI ordinarily could not be properly disclosed in compliance with HIP AA. This policy provides D&D 's policies and procedures with regard to the creation, use and disclosure of"De-identified data" and "Limited Data Sets."

Policy:

Whenever possible and appropriate, Workforce members should use and disclose PHI that is "De-identified" which means it does not or could not be used to identify an individual. "For purposes of research, public health and Health Care Operations only, D&D may disclose a "Limited Data Set." A "Limited Data Set" is PHI with certain direct identifiers removed regarding the individual, and the individual's relatives, employers and household members. The Privacy Officer makes the final determination as to whether certain information is De-identified, or may qualify as a limited data set. Questions regarding this policy should be directed to the Privacy Officer.

Procedure:

1. Only the Privacy Officer may determine if health information has been properly De-identified and must review and approve all De-identified information created as such by Workforce members.

2. Once information has been properly De-identified, it is no longer subject to HIPAA regulations, these policies and procedures or applicable law, provided that the conditions of this policy are met.

3. Information may be determined to be De-identified by a third party data expert or the information may be De-identified by removing the following data concerning the patient or the patient's relative, employers or household members:

    a. Names;
    b. Geographic identifiers smaller than a state, (e.g., street, city, count, zip code)
    c. All of dates (e.g., birth date, dates of service and date of death) and ages over 89;
    d. Telephone and fax numbers, and email addresses;
    e. Social security numbers, medical record numbers, health plan beneficiary numbers, and other account numbers;
    £ Certificate/license numbers;
    g. Vehicle identifiers and serial numbers, including license plate numbers;
    h. Device identifiers and serial numbers;
    i. Web Universal Resource Locators (URLS);
    j. Internet protocol (IP) Address numbers;
    k. Biometric identifiers, including voice and fingerprints, photographs, and other related images; and
    l. Any other unique identifying number, characteristic, or code, except for a "re-identification code."

m. D&D does not have actual knowledge that the remaining information could be used alone or in combination with other information to identify an individual.

4. For purposes of research, public health and Health Care Operations only. D&D may disclose a "limited data set." A "limited data set" is PHI with the following direct identifiers removed regarding the individual, and the individual's relatives, employers, and household members:

   a. Names;
   b. Address information other than city, town, state or zip code;
   c. Telephone and fax numbers;
   d. E-mail addresses, IP addresses and URLs;
   e. Social security numbers, medical record numbers, health plan beneficiary numbers, and other account numbers;
   f Vehicle identification and license plate numbers; and
   g. Biometric identifiers, including voice and fingerprints, photographs, and other related images.

5. If D&D discloses information for research, public health and Health Care Operations in the form of a limited data set, it will enter into a "data use agreement" with a recipient of the limited data set before using or disclosing a the information. This agreement shall ensure that the recipient will not use or disclose the data set information for other than these specific purposes. D&D Workforce members shall consult with the D&D counsel to obtain an approved data use agreement.

IX. Identifying, Reporting and Mitigating the Effect of an Unauthorized Release of PHI

Purpose:

A Covered Entity must take steps to mitigate any harmful effect that is known to it stemming from a use or disclosure of PHI in violation of its policies and procedures by the Covered Entity itself or its Business Associates, including a breach of the security of unsecured PHI. This policy is designed to give guidance and ensure compliance with all applicable laws and regulations related to mitigating the effect of the unauthorized release of information. Questions regarding this policy, or its application to a particular factual situation, should be directed to the Privacy Officer.

Policy:

1. D&D will take all necessary steps to mitigate any harmful effect that is known to D&D of a use or disclosure of PHI in violation of D&D policies and procedures. The Privacy Officer will, in consultation with legal counsel, preliminarily deal with any reported use or disclosure that violates these policies and procedures and determine appropriate actions and notifications.

2. Recognizing the importance of a breach of unsecured PHI, however, separate procedures have been developed. In the event of a breach of the security of unsecured PHI, the steps required by HIPAA (currently located at 45 C.F.R. Subpart D "Notification in the Case of Breach of Unsecured Protected Health Information") as amended or relocated from time to time, will be followed.

Procedures:

a. Use or Disclosure in Violation of Policies and Procedures.

1. In the event D&D discovers an improper use or disclosure of PHI in violation of its Policies; or is advised of such a violation, including advice by a member of its Workforce, another medical provider, a contractor of D&D (including a Business Associate), a patient or another third party, the individual Workforce member who receives the notification will immediately notify the Privacy Officer. If the potential breach is apparent and there are steps to take that can be taken immediately to stop the potential violation and/or mitigate the potential breach, the individual involved, in consultation with his/her immediate supervisor, should take those steps, even before advising the Privacy Officer. The Privacy officer will validate that there was a violation of D&D 's Policies, determine if a breach of unsecured PHI may have resulted, and direct the individual(s) involved and his/her (their) immediate supervisor as to the efforts to halt the improper use and/or disclosure, and to mitigate any harmful effects of the use and/or disclosure.

2. The Privacy Officer shall monitor remediation and notification of patients, the government, and media (as required) and shall ensure that appropriate discipline is applied if the breach has occurred as a result of an action or actions of a member or members of D&D's Workforce. The Privacy Officer will continue to monitor the situation and, in consultation with legal counsel as necessary, direct any further steps that need to be taken with regards to mitigation, notification, discipline, and prevention of further like incidents.

3. Upon initial notification, the Privacy Officer, in consult with D&D 's counsel if necessary, shall determine if any such improper use or violation constitutes a potential breach of unsecured PHI. If such a breach has occurred, the procedures of the following section will govern

b. Unsecured vs. Secured PHI

Procedures:

Breach of Unsecured Phi.

Notification is required if there is a breach and PHI is "unsecured." Conversely, notification is not required if there is a breach and PHI is "secured."

Secured PHI

PHI is considered secured if it meets the following standards:

- Electronic PHI, whether at rest in an electronic database or a device, or in motion (transmitted) outside the internal network of D&D, such as via the internet, should be secured by encryption consistent with HIPAA Guidelines.

- Discarded PHI, which includes discarded paper records or recycled electronic media, must have been destroyed in one of the following ways:

    - Paper, film, or other hard copy media must be shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction (i.e. whiting out or marking over the PHn is specifically not acceptable as a means of data destruction.

    - Electronic media have been cleared, purged, or destroyed consistent with HIPAA guidelines, such that the PHI cannot be retrieved.

- **D&D Personnel Reporting Requirements**

Generally, a breach has occurred if PHI is accessed, used or disclosed in a way that is not allowed under the HIPAA Privacy Rules. D&D personnel who discover, believe, or suspect that PHI has been accessed, used or disclosed in a way that violates the HIPAA Privacy Rules, should immediately report such information to the Privacy Officer.

D&D personnel who are determined to have failed to adhere to the policies and procedures regarding reporting of a breach of unsecured PHI will be subject to the disciplinary policies of D&D.

X. PHI Breach Determination and Notification Process: Overview of the Breach Determination and Notification Process Steps

The Privacy Officer, in consultation with legal counsel, will determine whether a breach of unsecured PHI has occurred and whether the incident triggers the notice requirements under HIPAA. The process for making this determination involve answering the following questions:

a. Breach Determination Steps

Step 1: Has PHI been used or accessed in a way that violates HIPAA?

Upon receiving a report of a potential breach, the Privacy Officer will review the report to determine whether there has been an access, use or disclosure of PHI that violates the HIPAA Privacy Rules.

Step 2: If yes, does the disclosure fall under a regulatory exception to the reporting requirement?

The Privacy Officer will consider, in consultation with D&D's legal counsel, whether the situation falls within an applicable exception to the definition of a breach which are listed below:

- Any unintentional acquisition, access, or use of PHI by D&D Workforce, if done in good faith and within the scope of authority, and which does not result in further use or disclosure in a manner not permitted under the Privacy Rule.

- Any inadvertent disclosure by a person authorized to access the PHI to another person authorized to access the PHI, and the PHI is not further used or disclosed in a manner not permitted under the Privacy Rule.

- Any disclosure where D&D 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.

If the answer to Step 2 is yes, the incident does not trigger notification requirements.

Step 3: If none of the three exceptions apply. the Privacy Officer, in consultation with D&D's legal counsel, will determine whether the improper use or access poses a low probability of compromising the data in question. To make this determination, the following factors must be applied:

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

- The unauthorized person who used the PHI or to whom the disclosure was made;

- Whether the PHI was actually acquired or viewed; and

- The extent to which the risk to the PHI has been mitigated.

If the answer to Step 3 is "No", D&D will follow the notification and reporting steps set forth below.

b. Notification and Reporting Steps:

If it is determined that: 1) a breach of unsecured PHI has occurred, 2) such breach compromises the privacy or security of the data; and 3) no exception to the reporting requirement applies, D&D will notify each individual whose unsecured PHI was subject to the breach. D&D will notify individuals without unreasonable delay, and in no case later than sixty (60) calendar days following discovery of the breach. The notice of breach to individuals will include the following information:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

- A description of the types of unsecured PHI involved in the breach;
- Any steps individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of the actions taken to investigate the breach, mitigate harm to individuals, and protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, which will include a toll-free telephone number, an e-mail address, web site, or postal address.

D&D will provide the notice in written form by first-class mail to the last known address of each individual, or may provide written notice by electronic mail, if the individual has agreed to receive electronic notices, and such agreement has not been withdrawn. If the affected individual is a minor or otherwise lacks legal capacity, the notification may be sent to the individual's Personal Representative. If the individual is deceased, the notice may be sent to the deceased individual's next of kin or Personal Representative if the address of the decedent's next of kin or Personal Representative is known.

If there is insufficient contact information for mail delivery to some or all affected individuals, individuals will be sent a substitute notice. The Privacy Officer should be consulted regarding the nature of such substitute notice as it will differ based on the number of individuals without sufficient contract information.

If it has been determined that the breach of unsecured PHI involved more than five hundred (500) residents of a particular state or jurisdiction smaller than a state, such as a county or city, D&D will notify a prominent media outlet of the breach. D&D will determine whether media notification is required and if so, will cause such notification to be made. Notification to media may be made by issuing a press release. Any press release shall be issued in consultation with D&D's public relations/media representative and/or D&D 's legal counsel.

D&D will notify the Department of Health and Human Services, Office of Civil Rights, of all breaches of unsecured PHI made by D&D personnel, either on no less than an annual basis for all breaches not previously reported in the preceding year or immediately, depending on how many individuals were affected by a breach.

If a breach of unsecured PHI involved more than five hundred (500) Individuals, D&D will notify Department of Health and Human Services, concurrently with the notification sent to an individual (without unreasonable delay but in no case later than sixty (60) calendar days following discovery of a breach).

Under the direction of the Privacy Officer, D&D will create and maintain a log of all breaches involving less than five hundred (500) individuals committed by D&D personnel. Within sixty (60) days after the end of each calendar year, D&D will submit the log to Department of Health and Human Services. D&D will also maintain the log and all other documentation regarding breach of unsecured PHI for ten (10) years. D&D is not required to submit information to Department of Health and Human Services, for breaches that occurred before September 23, 2009.

XI. Individual Right to File Complaints

Purpose:

Covered Entities are required to have mechanisms in place to accept complaints about any aspect of their practices regarding PHI. For example, individuals should be able to file a complaint when they believe that PHI relating to them has been used or disclosed improperly; that an employee of the entity has improperly handled the information; that they have wrongfully been denied access to or opportunity to amend the information; or, that the entity's notice does not accurately reflect its information practices. Questions regarding this policy, or its application to a particular factual situation, should be directed to the Privacy Officer.

Policy:

1. D&D will provide a process for individuals to make complaints concerning D&D's policies and procedures regarding the use or disclosure of PHI, or its compliance with such policies and procedures.

2. The Privacy Officer will be D&D 's designated contact for individuals to file complaints pursuant to this policy.

3. D&D will not require individuals to waive their rights to file a complaint with the Department of Health and Human Services as a condition of the provision of Treatment, Payment, enrollment in a health plan, or eligibility for benefits.

Procedure:

1. D&D will document all complaints received, and their disposition, if any, for a period of at least ten (10) years from the date of its creation or the date when it last was in effect, whichever is later.

2. The Privacy Officer should be contacted in order to file a complaint concerning D&D's policies and procedures required by the HIPAA Privacy Rule, or its compliance with such policies and procedures.

3. The name, or title, and telephone number of the contact person or office designated to receive complaints concerning D&D's policies and procedures required by the HIPAA Privacy Rule, or its compliance with such policies and procedures will be documented.

4. A form for filing a complaint is attached as Exhibit A, although all complaints will be investigated and responded to as set forth in this Policy, regardless of the form.

Exhibit A: Form for Filing HIPAA Complaint

Contact Person: _____

As required by the Health Information Portability and Accountability Act of 1996 (HIPAA) you have a right to complain about D&D Health's privacy policies, procedures or actions. D&D will not engage in any discriminatory or other retaliatory behavior against you because of this complaint. Please be as thorough and forthright as possible, and return it to the Contact Person listed above.

Please complete all of the sections below:

Name of Individual with the Complaint:_____ _

Address:_____ _

_____

Phone: _____

E-mail Address:_____ _

What is the best way to reach you?_____ _

What are the best hours to reach you?_____ _

Details of the complaint: (Please be as specific as possible with dates, times and the specific policy, procedure or action taken. Use the other side of this form if you need more room. Attach any relevant documents.)

_____

_____

_____

_____

Documents attached include:

- _____
- _____
- _____

Signature: _____ _ Date: _____ _

Print name: _____ _ Phone: _____ _

If not signed by the employee or spouse, please indicate relationship to the subject and provide your name:_____ _
. Your contact information should be provided above.

_____ parent or guardian of minor child
_____ guardian or conservator of an incompetent individual
_____ beneficiary or personal representative of deceased individual
other (specify)