Corteva Agriscience™
HIPAA Privacy Policies and Procedures

Originally Effective April 10, 2003 (Amended as of June 1, 2019)

These Policies and Procedures have been created in order for the Health Plans* (the “Health Plan”) to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and accompanying regulations and related legislation, as they pertain to health care privacy, security and transmission of electronic transactions. This revised document specifically includes updates to comply with the Health Information Technology for Economic and Clinical Health Act (HITECH). If any provisions of these Policies and Procedures are not compliant with HIPAA or a more restrictive state privacy law, the Policies and Procedures will be interpreted to comply with such law.

In general, the Privacy Rule permits the Health Plan, which has been determined to be a Covered Entity under HIPAA, to use or disclose protected health information (“PHI”) for certain limited purposes provided specific conditions are met. These Policies and Procedures set forth those purposes and conditions.

If you have questions about these Policies and Procedures, contact:
Kai Cole
HIPAA Privacy Official
For Corteva Agriscience Health Plans
Phone: (302) 999-6036
Email: Kai.Cole@corteva.com

* For this purpose, the Health Plans include: Medical Plan, Retiree Medical Program, Retiree Dental Plan, Dental Plan, Limited Purpose Health Care Spending Account Plan, and Vision Plan.
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Definitions</td>
<td>4</td>
</tr>
<tr>
<td>II. Health Plan Uses and Disclosures of Protected Health Information</td>
<td>7</td>
</tr>
<tr>
<td>A. Minimum Necessary Rule</td>
<td>7</td>
</tr>
<tr>
<td>B. Disclosure of a Limited Data Set for purposes of Research, Public Health or Health Care Operations</td>
<td>8</td>
</tr>
<tr>
<td>C. Uses and Disclosures for Research Purposes</td>
<td>10</td>
</tr>
<tr>
<td>D. Uses and Disclosures for Health and Safety Purposes</td>
<td>11</td>
</tr>
<tr>
<td>E. Uses and Disclosures Pursuant to Legal Proceedings and Law Enforcement</td>
<td>12</td>
</tr>
<tr>
<td>F. Uses and Disclosures Concerning Decedents</td>
<td>14</td>
</tr>
<tr>
<td>G. Uses and Disclosures for Other Government Purposes</td>
<td>14</td>
</tr>
<tr>
<td>H. Uses and Disclosures for Workers Compensation Purposes</td>
<td>15</td>
</tr>
<tr>
<td>I. Uses and Disclosures Only with Authorization</td>
<td>15</td>
</tr>
<tr>
<td>J. Disclosures to Individuals</td>
<td>17</td>
</tr>
<tr>
<td>K. Disclosures to Friends and Family Members</td>
<td>17</td>
</tr>
<tr>
<td>L. Disclosures to Secretary of Health and Human Services</td>
<td>18</td>
</tr>
<tr>
<td>M. Disclosures to Another Health Plan</td>
<td>18</td>
</tr>
<tr>
<td>N. Disclosures to Another Corteva Agriscience Benefit Plan, Other than a Health Plan</td>
<td>18</td>
</tr>
<tr>
<td>O. Disclosures to Another Health Plan</td>
<td>18</td>
</tr>
<tr>
<td>III. Safe-guarding Protected Health Information</td>
<td>19</td>
</tr>
<tr>
<td>A. Printed Materials</td>
<td>19</td>
</tr>
<tr>
<td>B. Facsimile Machines and Printers</td>
<td>20</td>
</tr>
<tr>
<td>C. Electronic Information</td>
<td>20</td>
</tr>
<tr>
<td>D. Telephonic and Other Verbal Communication</td>
<td>22</td>
</tr>
<tr>
<td>E. Office Safeguards</td>
<td>23</td>
</tr>
<tr>
<td>F. Breach Notification</td>
<td>23</td>
</tr>
<tr>
<td>IV. Health Plan Privacy Administration</td>
<td>24</td>
</tr>
<tr>
<td>A. Privacy Officer Appointed</td>
<td>24</td>
</tr>
<tr>
<td>B. Designating Authorized and Responsible Employees</td>
<td>24</td>
</tr>
<tr>
<td>C. Employee Training</td>
<td>24</td>
</tr>
<tr>
<td>D. Remedies for Violations of Protected Health Information Privacy Policies and Procedures</td>
<td>25</td>
</tr>
<tr>
<td>E. Reporting Policy Violations</td>
<td>26</td>
</tr>
<tr>
<td>F. Written Policies and Procedures</td>
<td>26</td>
</tr>
<tr>
<td>G. Record-keeping</td>
<td>26</td>
</tr>
<tr>
<td>H. Release of PHI to a Business Associate</td>
<td>28</td>
</tr>
<tr>
<td>V. Individuals’ Rights Regarding Protected Health Information</td>
<td>29</td>
</tr>
<tr>
<td>A. Privacy Notice</td>
<td>29</td>
</tr>
<tr>
<td>B. Access to Protected Health Information</td>
<td>30</td>
</tr>
<tr>
<td>C. Request for Restriction on Uses and Disclosures</td>
<td>31</td>
</tr>
<tr>
<td>D. Confidential Communication</td>
<td>32</td>
</tr>
<tr>
<td>E. Amendment of Protected Health Information</td>
<td>32</td>
</tr>
<tr>
<td>F. Accounting</td>
<td>33</td>
</tr>
<tr>
<td>G. Complaints</td>
<td>35</td>
</tr>
<tr>
<td>H. Personal Representatives</td>
<td>35</td>
</tr>
</tbody>
</table>
VI. Exhibits

A. Group Health Plan Employees ........................................................................ 37
B. HIPAA Forms .................................................................................................. 38
C. Privacy Notice ................................................................................................ 39
I. **Definitions**

- **Authorization** – an Individual’s specific written permission, as described in Policy Section II.I, to the Health Plan to use and disclose PHI for purposes other than Treatment, Payment or Health Care Operations and other specified purposes described in Policy Sections II.C through II.H.

- **Business Associate** – a person or entity, other than an employee, who performs or assists in the performance of a function or activity involving the use or disclosure of PHI on behalf of the Health Plan. Such functions or activities include claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, repricing, and other professional services.

- **Covered Entity** - means a health plan, a health care clearinghouse, or a health care carrier who transmits any health information in electronic form in connection with a transaction covered by the HIPAA electronic transaction regulations.

- **Corporate Records and Information Management (CRIM)** - Corteva Agriscience’s official policy for record retention. Further details are found [https://agcompany.sharepoint.com/teams/CRIMDuPontSite/default.aspx](https://agcompany.sharepoint.com/teams/CRIMDuPontSite/default.aspx).

- **De-identified PHI** - health information that: (i) does not include any of the following identifiers of the Individual or the Individual’s relatives, employers, or household members: names, geographic subdivisions smaller than a state, month and day of birth and other personal dates (including admission and discharge), telephone and fax numbers, electronic mail addresses, social security number, medical record numbers, health plan beneficiary numbers, account numbers, certificate or license numbers, vehicle identifiers (including serial and license plate numbers), device identifiers and serial numbers, Web universal resource locators, Internet procedures address numbers, biometric identifiers, full-face photographic images, and any other unique identifying number, characteristic, or code; or (ii) for which it has been statistically determined that an Individual cannot be identified from the information provided.

- **Designated Record Set** – a record that includes PHI maintained by or for the Health Plan that pertains to enrollment, payment, claims adjudication, case management, and other information used to make Health Plan related decisions about Individuals. The Designated Record Set includes an Individual’s enrollment records, contribution amounts paid by Corteva Agriscience and the Individual for coverage under the Group Health Plan, Explanations of Benefits or other claims records, records of any appeals, and medical management records.

- **Electronic Transaction Regulations** - the HIPAA regulations which address the electronic transmission of health information, 45 C.F.R. Parts 160 and 162.

- **Group Health Plan (GHP) Employee** – an employee whose duties require access to PHI for purposes of Health Plan administration. This includes such responsibilities as receiving enrollment information, communicating PHI to insurance carriers or Business Associates, assisting an Individual in resolving a disputed claim, communication with an Individual
regarding coverage questions where PHI is discussed, and other Health Plan related administration.

- **Health Care Operations** – any of the following activities to the extent that they are related to the Health Plan’s functions:

1. Conducting quality assessment and improvement activities; population-based activities related to health improvement, reduction of health care costs, case management and care coordination, contacting health care carriers and patients regarding treatment alternatives; and related functions that do not include treatment;

2. Reviewing competence or qualifications of health care carriers, evaluating carrier and plan performance;

3. Underwriting and other activities that relate to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance);

4. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

5. Business planning and development, such as cost-management and planning-related analyses related to managing and operating the Health Plan, and development or improvement of coverage policies; and

6. Business management and general administrative activities including but not limited to:
   (i) management activities related to implementation of and compliance with the requirements of the Privacy Rule, (ii) resolution of internal grievances, (iii) due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the successor in interest is or will become after the sale a Covered Entity, and (iv) consistent with applicable requirements of the Privacy Rule, creating de-identified health information and marketing for which an individual authorization is not required.

- **Health Plans** – collectively, the employee benefit programs sponsored by Corteva Agriscience that provide health care coverage for employees and dependents, including: medical, retiree medical, dental, retiree dental, employee assistance, flexible spending account, and vision programs. The Health Plan is a Covered Entity under HIPAA.

- **HIPAA Privacy Official** – is the chief employee accountable for developing, implementing and updating the Health Plans’ privacy policies and procedures.

- **Individual** – a person covered by the Health Plan or a decedent previously covered by the Health Plan who is the subject of PHI. This includes an employee and his spouse and dependents or a retiree.
• **Payment** – activities undertaken by the Health Plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits, including: determination of eligibility or coverage, adjudicating benefit claims, underwriting, billing and collection, and utilization review.

• **Personal Representative** - a person entitled under applicable law to decide and act on behalf of an Individual with respect to the Individual’s health care. Such Personal Representative is treated as the Individual under these policies and procedures except as specified under Policy Section V.H.

• **Privacy Rule** – means regulations and accompanying guidance implementing requirements of HIPAA, including specifically the rules at 45 C.F.R, Part 164, Subpart E.

• **Protected Health Information (PHI)** – means individually identifiable health information that relates to the past, present, or future physical or mental condition of an Individual, provision of health care to an Individual, or payment for such health care.

• **Qualified Protective Order** – means an order of a court or an administrative tribunal or a stipulation by the parties that prohibits the parties from using or disclosing PHI for purposes other than the underlying litigation or proceeding for which the records are requested and requires the return to the Health Plan or destruction of the PHI at the end of the litigation or proceeding.

• **Required by Law** - has the meaning included in regulations issued under HIPAA, and means a mandate contained in law that compels the entity to use or disclose PHI and that is enforceable in court; including court orders and court-ordered warrants; subpoenas issued by a court, governmental inspector or administrative body authorized to require production of information; a civil investigative demand; Medicare conditions of participation; and regulations requiring information as a condition of receiving public benefits.

• **Security Rule** - means regulations and accompanying guidance implementing requirements of HIPAA, including specifically the rules at 45 C.F.R, Part 164, Subpart C.

• **Summary Health Information** – means health information which may identify an Individual and that summarizes the claims history, claims expenses, or type of claims experienced by Individuals who are participants in the Health Plan, and which fits the definition of De-Identified PHI, except that the geographic information need only be aggregated to the level of a five-digit zip code.
II. Health Plan Uses and Disclosures of Protected Health Information

The Health Plan will use or disclose PHI only in the following circumstances:

1. to carry out Treatment, Payment or Health Care Operations of the Health Plan;
2. in accordance with an Individual’s Authorization (Policy Section II.1.);
3. or as otherwise specifically permitted by this Section.

A. Minimum Necessary Rule

No employees, other than GHP Employees should have access, accept receipt, record or transmit PHI, other than PHI that relates directly to that employee as an Individual or as permitted by an Authorization or as otherwise specifically permitted by this Section. Group Health Plan Employees are listed in Exhibit A.

When using, disclosing, or requesting PHI, GHP Employees must make reasonable efforts to limit such PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. For example, Corteva Agriscience Integrated Health may not use, disclose, or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request.

In addition to limiting the PHI used or disclosed, GHP Employees must take steps to ensure that only the person(s) needing the PHI for her job responsibilities receives it. This duty applies regardless of whether such recipients are other GHP Employees, Business Associates, or other persons to whom the GHP Employee is required, permitted, or authorized to disclose PHI. If a GHP Employee is the recipient of PHI, that employee should attempt to process, copy, or record such PHI without disclosing it to others, unless such disclosure is necessary.

Prior to any disclosure of PHI, the GHP Employee must verify the identity and authority of the person requesting such information, if not already known to the GHP Employee.

Example 1: If disclosure is to a public official, verification will be made in-person by viewing an identification badge that indicates proper authority or, if not in-person, by receipt of written authorization statement on appropriate letterhead. Example 2: If disclosure is to a person who the GHP Employee does not recognize, verification will be made by inspecting an identification document. Example 3: If disclosure is made through a telephone call, and the GHP Employee does not recognize the Individual caller, the GHP Employee should require the person to provide identifiable information (i.e. last four digits of the social security number, date of birth (month and day), address, etc.). If an additional document or statement is required under these Policies and Procedures for the specific disclosure, the GHP Employee must obtain such document or statement prior to making the disclosure.

Routine Uses. For routine uses and disclosures of PHI (e.g. enrollment, premium collection and payment, and change-in-status notification), the following procedures apply:

- Forms will request only that information which is minimally necessary to accomplish the function. See Exhibit B for HIPAA Forms.
• Processing will involve only the GHP Employee(s) needed to complete the transaction or transmittal.
• Transmittal will be limited to no more information than minimally necessary to accomplish the function.

Non-routine Uses. For any non-routine disclosure request (e.g., related to a benefit claim resolution or coverage exclusion exception), the same procedures apply, but must be implemented taking into account the specific purpose of the request.

Minimum Necessary does not apply. The minimum necessary rule does not apply to the following circumstances:

1. disclosure to a health care provider for treatment;
2. disclosure to the Individual;
3. disclosures to the Secretary of Health and Human Services;
4. uses and disclosures Required by Law (as defined in the Privacy Rule); and
5. uses and disclosures for which the Individual gave Authorization.

Reliance on a request for information. The Health Plan will rely on another party’s requested disclosure as the minimum necessary for the stated purpose, if such reliance is reasonable under the circumstances, and

• the disclosure is to a public official who represents that the information requested is the minimum necessary for the stated purpose(s);
• the information is requested by another Covered Entity;
• the information is requested by another GHP Employee or a Business Associate of the Health Plan for the purpose of providing professional services to the Health Plan, and there is a representation that the information requested is the minimum necessary for the stated purpose(s); or
• the request is made for research purposes (for example, epidemiology) and appropriate documentation and representations have been provided.

B. Disclosure of a Limited Data Set for purposes of Research, Public Health or Health Care Operations.

A GHP Employee may use or disclose a Limited Data Set as long as the HIPAA Privacy Official or her designee enters into a Data Use Agreement with the Limited Data Set recipient, and such Data Use Agreement complies with the requirements listed below.
**Limited Data Set definition:** A Limited Data Set is PHI that excludes the following identifiers of the Individual or of relatives, employers or household members of the Individual:

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

**Data Use Agreement definition:** A GHP Employee may use or disclose a Limited Data Set only if it obtains satisfactory assurance, in the form of a Data Use Agreement which contains the following provisions:

1. Establish the permitted uses and disclosures of such information by the Limited Data Set recipient;
2. The Data Use Agreement may not authorize the Limited Data Set recipient to use or further disclose the information in a manner that would violate the requirements of this policy section, if done by the Health Plan;
3. Establish who is permitted to use or receive the Limited Data Set; and
4. Provide that the Limited Data Set recipient will:

(a) Not use or further disclose the information other than as permitted by the Data Use Agreement or as otherwise required by law;

(b) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the Data Use Agreement;

(c) Report to the HIPAA Privacy Official any use or disclosure of the information not provided for by its Data Use Agreement of which it becomes aware;

(d) Ensure that any agents, including a subcontractor, to whom it provides the Limited Data Set agrees to the same restrictions and conditions that apply to the Limited Data Set recipient with respect to such information; and

(e) Not identify the information or contact the Individuals.

The Data Use Agreement shall be maintained by the HIPAA Privacy Official or her designee and shall be retained in accordance with Policy Section IV.G.

**Corteva’s Compliance Duty** - A GHP Employee is not in compliance with this policy section if he or she knows of a pattern of activity or practice of the Limited Data Set recipient that constitutes a material breach or violation of the Data Use Agreement, and the GHP Employee takes no reasonable steps to inform the HIPAA Privacy Official, to cure or end the breach or violation. If the GHP Employee does take steps to cure the breach or end the violation and such steps are unsuccessful, then the GHP Employee must do the following:

(a) Discontinue disclosure of PHI to the recipient; and

(b) Report the problem to the Secretary (of Health and Human Services).

C. Uses and Disclosures for Research Purposes

The GHP is permitted to use and disclose protected information for research purposes (including epidemiology analysis conducted by Corteva Agriscience), provided the GHP obtains a waiver or alteration of an authorization for the use and disclosure as approved by the Institutional Review Board (IRB) or privacy board (as defined in the Privacy Rule). The waiver or alteration documentation must include:

1. the date of approval of the waiver or alteration

2. information indicating:
   i. the use or disclosure of PHI involves no more than minimal risk
   ii. the alteration or waiver will not adversely affect the rights and welfare of the individual
iii. the research could not practicably be conducted without it

iv. the research could not be practicably conducted without access and use of PHI

v. the privacy risks to Individuals whose PHI is to be used or disclosed are reasonable in relation to anticipated benefits or the knowledge expected to result from the research

vi. there is an adequate plan to protect identifiers from improper use and disclosure

vii. there is an adequate plan to destroy identifiers at the earliest opportunity, unless there is a health or research justification for retaining the identifiers, or such retention is required by law

3. a written agreement from a person or entity receiving PHI not to reuse or disclose PHI to any other person or entity except as required by law, for authorized oversight or a research project, or for other research for which use and disclosure of PHI would be permitted

4. a description of PHI for which the use or access has been determined to be necessary for the research

5. a signature by the chair of the IRB or privacy board, or a member of the IRB or privacy board who is designated by the chair to sign documentation

6. a statement identifying the IRB or privacy board that approved the waiver/alteration

7. a statement that the waiver has been reviewed and approved under review procedures described in the Privacy Rule.

D. Uses and Disclosures for Health and Safety Purposes

All uses and disclosures for health and safety purposes must first be authorized by the HIPAA Privacy Official, or his designee:

1. Threat to Health or Safety.

A GHP Employee will use or disclose PHI to prevent or lessen serious, imminent threat to the health or safety of a person or the public if made to someone who can prevent or lessen the threat. A GHP Employee must not, however, use or disclose PHI if the information was learned through a request by the Individual to initiate or be referred for treatment, counseling, or therapy to address the Individual’s propensity to commit a crime.

2. Abuse, Neglect, or Domestic Violence.

If an Individual is a victim of abuse, neglect, or domestic violence, a GHP Employee will disclose PHI to a government authority authorized by law to receive such reports. Except instances of child abuse or neglect, such disclosure must meet at least one of the following conditions:

(a) disclosure is made only to the extent required by a law;
(b) the Individual agrees to the disclosure; or

(c) the disclosure is expressly authorized by a law or regulation and either (i) the disclosure is necessary to prevent serious harm to the Individual or others or (ii) the Individual is unable to agree to the disclosure because he or she is incapacitated but, according to an official authorized to receive the disclosure, it is necessary for immediate enforcement activity and it will not be used against the Individual.

In instances of abuse, neglect, or domestic violence not involving a child, the GHP Employee must inform the Individual of the disclosure unless (i) doing so would put the Individual at risk of serious harm, or (ii) the GHP Employee would be informing the Individual’s Personal Representative and the Personal Representative is believed to be responsible for the abuse, neglect, or other injury.

If the abuse, neglect, or domestic violence does involve a child, none of the conditions (a), (b), or (c) above needs to be met. Also, in such instances, the GHP Employee need not inform the Individual of the disclosure.

3. Public Health Activities.

An GHP Employee may use or disclose PHI (a) to a public health authority authorized by law to collect or receive such information for prevention purposes (e.g., disease, injury, or disability), (b) to a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect, or (c) to a person subject to jurisdiction of the Food and Drug Administration under limited circumstances (i.e., to track product defects or improper labeling).

4. Health Oversight Activities.

A GHP Employee may use or disclose PHI to a health oversight agency for oversight activities authorized by law (including audits, investigations or inspections) or other activities necessary for appropriate oversight of the health care system, and of government programs and entities subject to civil rights laws that require health information. Health oversight activities do not include investigations or other activities in which the Individual is the subject of that investigation or activity unless it arises out of and is related to the receipt of health care, a claim for public health benefits, or eligibility for or receipt of public benefits or services related to a patient’s health.

E. Uses and Disclosures Pursuant to Legal Proceedings and Law Enforcement

All uses and disclosures for legal and law enforcement purposes must first be authorized by Corteva Agriscience Legal (Lori Knauer).

1. Legal Proceedings with Court Order.
A GHP Employee will, to the extent ordered, disclose PHI in the course of a judicial or administrative proceeding in response to an order from a court or an administrative tribunal.

2. Legal Proceedings without Court Order.

Absent a court order, disclosure of PHI will be made in response to a subpoena, discovery request, or other legal process provided one of the following conditions is met:

(a) the GHP Employee receives documentary evidence that (i) the requesting party provided or made a reasonable attempt to provide written notice to the Individual (including sufficient information to enable the Individual to raise an objection), (ii) the time for raising an objection has elapsed, and (iii) either no objection was raised or all objections have been resolved by the Court in a way that permits the disclosure; or

(b) the GHP Employee receives documentary evidence that the requesting party obtained or made a reasonable attempt to obtain a Qualified Protective Order (i.e., an agreed Qualified Protective Order has been presented to the court or the requesting party has sought such an order from the court or tribunal); or

(c) the Health Plan itself makes reasonable efforts to notify the Individual (as described in (a) above) or to obtain a Qualified Protective Order (as described in (b) above).

3. Law Enforcement.

A GHP Employee will disclose PHI to a law enforcement officer for law enforcement purposes, provided the following conditions are met, if applicable:

(a) Court Orders. The disclosure is required by law or is in compliance with a court order (including court-ordered warrant, subpoena, or summons), a grand jury subpoena, or an administrative request, provided (i) the information requested is relevant and material to a legitimate law enforcement inquiry and is limited to the purpose of that inquiry, and (ii) De-identified Information could not reasonably be substituted for the PHI.

(b) Suspects, Missing Persons, etc. The disclosure is in response to a law enforcement officer’s request, and is for the purpose of locating a suspect, fugitive, material witness, or missing person and the disclosure is limited to following information:

- name and address,
- date and place of birth,
- social security number,
- ABO blood type and rh factor,
- type of injury,
- date and time of treatment,
- date and time of death, and
• distinguishing physical characteristics.

(c) **Crime Victims.** The disclosure is in response to a law enforcement officer’s request for information about an Individual who is a suspected crime victim and the Individual/victim agrees to the disclosure. If the Individual/victim is unable to agree to the disclosure because of incapacity or emergency circumstances, the GHP Employee will make the disclosure only if the law enforcement official represents that (i) the disclosure is necessary to determine if someone other than the Individual/victim committed a crime (ii) it is necessary for immediate enforcement activity, and (iii) it will not be used against the Individual/victim, and (iv) the disclosure is in the Individual’s/victim’s best interests.

(d) **Crime Related to Individual’s Death.** The disclosure is made to a law enforcement officer and is about a deceased Individual whose death may have resulted from a crime. (See also Policy Section II.F., below.)

(e) **Crime on Premises.** The disclosure is made to a law enforcement officer and is evidence of a crime that occurred on Corteva Agriscience’s premises.

**F. Uses and Disclosures Concerning Decedents**

All uses and disclosures concerning decedents must first be authorized by the HIPAA Privacy Official, or his designee.

1. **Post-mortem Identification, etc.**

A GHP Employee will use or disclose PHI to (a) a coroner or medical examiner for purposes of identifying the decedent, determining cause of death, or other lawful purpose or (b) a funeral director as necessary for purposes of carrying out his duties. (If the requested disclosure is to a law enforcement officer and is about a deceased Individual whose death may have resulted from a crime, see Policy Section II.C.3(d), above.)

2. **Tissue Donation.**

A GHP Employee will use or disclose PHI for purposes of cadaveric organ, eye, or tissue donation to organizations engaged in procuring, banking, or transplanting such cadaveric organs, eyes, or tissues.

**G. Uses and Disclosures for Other Government Purposes**

All uses and disclosures for Government Purposes must first be authorized by Corteva Agriscience Legal.

Once authorized, a GHP Employee will use or disclose PHI under the following special circumstances:
1. Armed Forces.

A GHP Employee may use or disclose PHI about Individuals who are members of the Armed Forces (including foreign military authorities) for activities necessary to assure proper execution of military mission, provided that, for the United States, the appropriate military authority has published a notice in the Federal Register that includes appropriate military command authorities and permitted purposes for the use or disclosure.


A GHP Employee may use or disclose PHI to authorized federal officer for intelligence, counter-intelligence, or other national security activities authorized by the National Security Act.


A GHP Employee may use or disclose PHI to an authorized federal officer for the provision of protective services to the President or others authorized by 18 U.S.C. 3056, foreign heads of state or others authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

4. Correctional Institution or Lawful Custody.

A GHP Employee may use or disclose PHI to a correctional institution or law enforcement officer who has lawful custody of the Individual if the information is necessary for provision of health care to the Individual or for ensuring the Individual’s, other inmates’, or correctional institution employees’ health or safety.

H. Uses and Disclosures for Workers Compensation Purposes

All uses and disclosures for workers compensation purposes must first be authorized by the HIPAA Privacy Official, or her designee. Once authorized, a GHP Employee will use or disclose PHI for compliance with workers compensation and similar laws that provide benefits for work-related injuries or illnesses without regard to fault to the extent necessary for such compliance.

I. Uses and Disclosures Only With Authorization

The Health Plan will not use or disclose PHI for reasons other than treatment, payment, or health care operations of the Health Plan, and - less frequently - other purposes specifically described in this Section. For all other uses and disclosures, the Health Plan must obtain the Individual’s Authorization prior to the use and disclosure and each such use or disclosure must be consistent with the Authorization given for that use or disclosure. See the form and instructions in Exhibit B.
An Authorization is not valid unless it contains all of the following elements:

1. a description of the PHI to be used or disclosed;

2. the name or job titles of the person(s) authorized to make the use or disclosure described;

3. the name or job titles of the person(s) to whom the disclosure may be made;

4. a description of each purpose of the requested use or disclosure or a statement that it is at the request of the Individual;

5. an expiration date or expiration event related to the Individual or to the purpose of the use or disclosure (i.e. when the person’s participation in a Health Plan terminates);

6. a statement of the Individual’s right to refuse to sign the Authorization;

7. if the Health Plan conditions eligibility or enrollment on the signing of an Authorization, a statement of such condition;

8. a statement of the Individual’s right to revoke and a description of the procedure for the Individual to revoke the Authorization;

9. a statement that the PHI might be further disclosed by the recipient and might not thereafter be protected by the Privacy Rule; and

10. the Individual’s signature or that of his Personal Representative together with a description of that Personal Representative’s authority to act on behalf of the Individual.

An Authorization may be sought as a condition for enrollment in the Health Plan for purposes of determining eligibility for benefits under the Health Plan or for its underwriting or risk rating determinations; however, such Authorization does not apply to the disclosure of psychotherapy notes. An Authorization may be sought solely for the purpose of creating PHI for disclosure of the PHI to a third party. For example, if an employment physical is required by Corteva Agriscience, and as a condition of employment the employee will be required to turn over these medical records to Corteva Agriscience. Those records will not be able to be obtained from a covered health care carrier, without first obtaining an Authorization from the employee. Thus, employment may be conditioned on an employee providing an Authorization which requires a covered health care carrier to turn these records over to Corteva Agriscience.

An Individual will sign an Authorization to permit use of PHI to determine an appeal, including a separate Authorization for any psychotherapy notes.
Each signed Authorization must be given to the HIPAA Privacy Official who will retain the Authorization for a period of at least **six years** from the later of (a) the effective date or (b) expiration date, if any. The HIPAA Privacy Official, or her designee, will provide the Individual with a copy of the Authorization.

An Individual may revoke an Authorization in writing at any time except to the extent that the Health Plan already has acted in reliance on the Authorization or, if the Authorization was a condition for enrollment under an insurance contract, where the insurer has the legal right to contest a claim. The Individual must deliver the written revocation to the HIPAA Privacy Official who will notify the relevant GHP Employee(s) and retain the revocation for a period of at least **six years** from its effective date.

### J. Disclosures to Individuals

A GHP Employee must disclose an Individual’s own PHI to the Individual when requested by the Individual, except information compiled in reasonable anticipation of or use in legal proceedings.

### K. Disclosures to Friends and Family Members

The Health Plan will only disclose an Individual’s PHI to another person if the Health Plan has a written Authorization from that Individual permitting it to make such disclosure. Under limited circumstances the Health Plan will disclose PHI to a family member, close personal friend, or other person identified by the Individual without Authorization. Such disclosure is limited to PHI that is directly relevant to that person’s involvement with the Individual’s care or payment for health care where **at least one** of the following conditions also is met:

1. The Individual agrees to the disclosure;
2. the Individual had an opportunity to agree or object to the disclosure and did not object;
3. based on professional judgment and the circumstances, it can reasonably be inferred that the individual did not object to the disclosure; or
4. if the Individual was not available to agree or object or cannot agree or object due to the Individual’s incapacity (i.e. due to an emergency situation), but the disclosure is in the Individual’s best interest.

Opportunity to object, for these purposes, means the Individual was present or otherwise available prior to the disclosure and had the capacity to make health care decisions.

The Health Plan also may use or disclose PHI to notify or assist in the notification of a family member, Personal Representative, another person responsible for the Individual’s care,
or a disaster relief organization of the Individual’s location, condition, or death provided (1), (2), (3) or (4) above is satisfied.

L. Disclosures to Secretary of Health and Human Services

A GHP Employee must disclose PHI to the Secretary of Health and Human Services when requested by the Secretary of Health and Human Services for purposes of determining the Health Plan’s compliance with the Privacy Rule.

M. Disclosures to Another Health Plan

A GHP Employee may disclose an Individual’s PHI to another Health Plan (i.e., another GHP Employee with respect to that plan) as long as the disclosure is for Payment or Health Care Operation purposes, and only the minimum necessary is disclosed. If the disclosure is for other than Payment or Health Care Operation purposes, an Authorization first must be obtained from the Individual.

N. Disclosures to Another Corteva Agriscience Benefit Plan, Other than a Health Plan

A GHP Employee may only disclose PHI to a non-Health Plan (i.e., another Corteva Agriscience employee with responsibility for that non-Health Plan, such as a disability or long-term care plan) if it first receives an Authorization from the Individual or as otherwise specifically permitted under this Section (for example, to comply with worker’s compensation law requirements). If possible, de-identified health information should be used instead of PHI.

O. Disclosures to Corteva Agriscience

GHP Employees will disclose PHI to Corteva Agriscience only in accordance with this Policy and the provisions of the Health Plans, as amended to comply with HIPAA.
III. **Safe-guarding Protected Health Information**

The HIPAA Privacy Official and other GHP Employees must take reasonable steps to ensure that PHI is not intentionally or unintentionally used or disclosed in any manner not consistent with these privacy policies. Such steps include securing PHI using administrative, physical and electronic access barriers, destroying documents containing PHI that do not need to be retained (see Policy Section IV.G regarding record-keeping), training GHP Employees regarding privacy policies (see Policy Section IV.C regarding such training), and limiting the number of persons included as GHP Employees. Physical access to areas containing PHI will be limited, wherever possible, to GHP Employees only. GHP Employees should keep PHI in separate files from personnel files or other non-PHI file. The following procedures apply:

**A. Printed Materials.**

GHP Employees must store all printed materials containing PHI in secure locations when not in use. For example, PHI should be stored in locked filing cabinets, desk drawers, or rooms to which only a GHP Employee has physical and administrative access. A GHP Employee will not store PHI in an Individual’s personnel file. When in use, the GHP Employee must take reasonable steps to ensure that such printed materials are viewable only by the GHP Employee. For example, if the GHP Employee has PHI in printed material on his or her desk, he or she should put away the material before leaving his or her desk for any amount of time. At no time will the files remain unlocked when the GHP Employee has left the office premises. If a GHP Employee needs to remove a file containing PHI from the office premises, that GHP Employee will maintain such file in a secure location and use all necessary steps to maintain the confidentiality of the information.

Mail addressed to GHP Employees who regularly receive mail-containing PHI should be unsealed only by that addressee. Mail should be left in a mail slot belonging only to that GHP Employee. If a GHP Employee knows that an Individual will be sending PHI to her through the mail, the GHP Employee will instruct that Individual to send the information to her attention and to mark the envelope “Confidential.” If a GHP Employee is sending PHI to an Individual, she shall mark the envelope “Confidential” and shall verify the Individual’s address prior to mailing it.

In case of a fire, vandalism, or a natural disaster emergency and disaster recovery will be conducted in accordance with Corteva Information Security policies.

If printed material no longer needs to be retained after use, it should be shredded or otherwise destroyed by the GHP Employee, unless subject to Policy Section IV.G regarding record-keeping. Members of the Benefit Plan Appeals Committee will destroy any printed copies of PHI after a determination is made on the Individual’s appeal.
B. Facsimile Machines and Printers.

GHP Employees must take reasonable steps to ensure that all incoming facsimiles and print jobs containing PHI are viewable and retrievable only by the GHP Employee with a legitimate need to know. All PHI must be transmitted via e-fax (Efaxsend or similar product supported or permitted by Corteva Agriscience). A GHP Employee who transmits a facsimile will take reasonable steps to verify that the intended recipient is a person to whom the GHP Employee is required, permitted, or authorized to disclose PHI as described in Policy Section III.B. When possible, all fax machines shall be secured during non-working hours.

The Confidential Fax Cover Sheet should be used for all communications of PHI. The Notice of Misdirected Fax should be used whenever PHI has been sent to the wrong fax machine. Fax machines must be secured within an area where only those who are GHP Employees will have access or the sender will ensure the recipient will be physically waiting by the fax machine and confirm receipt verbally. Notice should be given to non-GHP Employees to view coversheets only to identify the correct recipient. PCs with fax software should be configured so that incoming calls to the modem will only interface with the fax software.

If a fax or copy no longer needs to be retained after use, it should be shredded, unless subject to Policy Section IV.G regarding record-keeping.

If a fax or copy-containing PHI is retrieved by someone other than the GHP Employee, that person will not read the contents of such fax except to determine the intended recipient. If a GHP Employee knows that an Individual will be sending PHI to him or her through a fax, the GHP Employee will instruct that Individual to send the information to her attention and to mark the fax “Confidential”. A GHP Employee must not communicate PHI regarding an employee’s spouse or child to that employee, unless the GHP Employee receives a signed Authorization from that spouse or child prior to the disclosure. The GHP Employee also must not disclose an Individual’s PHI to another person, unless that other person is the Personal Representative of the Individual (See Policy Section V.G) or as otherwise specifically permitted under this Policy.

Users who can’t send PHI to a secure printer will either send the document to the printer in a locked format or wait by the printer until the print job is complete, then remove PHI immediately from the printer. Users copying PHI will ensure that all copies and all originals are removed before leaving the area. When a copier malfunctions, all “miscopies” that contain PHI will be destroyed appropriately.

C. Electronic Information.

HHS has adopted specific regulations governing security of electronic PHI (“ePHI”). These rules require the Health Plan to ensure the confidentiality, integrity and availability of all ePHI the Health Plan creates, receives, maintains or transmits.
There are five primary categories in which the GHP Employees access ePHI:

1. Data warehouse;
2. Plan Sponsor database;
3. HCM archive databases;
4. Payroll systems;
5. Emails containing information on Health Plan appeals, including second opinions from doctors and case management information.

The HIPAA Privacy Official is responsible for maintaining procedures governing access to the data warehouse and databases. These procedures describe methods for approving users of the database, installing and removing any software necessary to access these databases, removing users upon job termination or role change, and monitoring usage of the database.

The data warehouse and databases are maintained by entities other than Corteva Agriscience, and Corteva Agriscience has entered into contracts with these entities requiring them to take appropriate steps to maintain the integrity and availability of the information held in them. In some cases, Corteva Agriscience has also entered into Business Associate Contracts with the entities.

Corteva Agriscience Information Security Organization maintains comprehensive rules governing protection and security of all information held and used by Corteva Agriscience employees and contractors, including electronic information. Corteva Information Security has classified ePHI as subject to its “Highest Risk” classification, which carries specific security controls and requirements.

In addition to Corteva Information Security requirements, GHP Employees shall also follow the following rules.

GHP Employees must take reasonable steps to ensure that access to electronically transmitted PHI is password protected. Electronically-stored PHI, including such information residing in electronic mail messages, electronic document files, databases, external storage devices and other computer files must be password-protected and accessible only by a GHP Employee who has a need for access. A GHP Employee also must take reasonable steps to ensure that PHI displayed on his or her monitor is viewable only by the GHP Employee. For example, if the GHP Employee has PHI displayed on his computer screen, he or she should close the window containing the PHI before leaving his desk for any amount of time. Password protected screen savers should be utilized when the computer is not being used (pursuant to the existing Corteva Information Security policy). If screen saver is not password protected, then the computer must be shut down. All GHP Employees must log off their computers any time they leave the office premises.
All portable storage media containing PHI shall be kept in a locked drawer. If a GHP Employee needs to remove a laptop or external storage device containing PHI from the office premises, that GHP Employee will maintain the laptop and/or external storage device in a secure location and use all necessary steps to maintain the confidentiality of the information.

Any electronic materials containing PHI should not be downloaded to hard drives.

Email containing PHI must be encrypted. For internal Corteva Agriscience Email, Outlook must be used and attachments must be encrypted and password protected. For external Email, a Corteva approved encryption method must be used.

For misdirected Email, recipient should reply to sender and delete Email. Misdirected Email should not be forwarded to intended recipient.

If the information or file no longer needs to be retained after use, it should be deleted, unless subject to Policy Section IV.G regarding record keeping.

All GHP Employees shall follow Corteva Information Security policies regarding back-up of information. Third parties maintain the data warehouse, plan sponsor and payroll database, so loss of access by Corteva Agriscience will not harm integrity of original source of information.

Periodically the HIPAA Privacy Official will meet with representatives from Corteva Information Security to review this Privacy Policy and Corteva Information Security policies applicable to ePHI. The review will include audits conducted by Corteva Information Security of adherence to Corteva Information Security policies (such as login anomaly and exception reports, security incident reports) and a review of all policies and procedures to make sure they continue to be current in light of any changes in technology or administrative procedures.

D. Telephonic and Other Oral Communication.

GHP Employees must take reasonable steps to ensure that telephone and other verbal conversations in which PHI is discussed are not overheard by persons who do not have a legitimate need to know the content of the conversation. For example, conferences in which PHI is discussed generally should be conducted in a closed room. If a conversation where PHI is discussed is conducted in a cubicle, the GHP Employee will speak in a manner not to be overheard by others. At no time should GHP Employees converse about PHI in a place where others who do not have a need to know such information may overhear.

PHI should not be included in phone messages to individuals. Only the minimum information necessary to return the call should be relayed.

A GHP Employee must not communicate PHI regarding an employee’s spouse or child to that employee, unless the GHP Employee receives a signed Authorization from that spouse or child prior to the disclosure.

When receiving a voice message, GHP Employee should not put the phone on speaker, unless there are other GHP Employees who need to hear the message in order to perform their job or a necessary function.
When speaking with an Individual on the phone about PHI, the GHP Employee will take proper steps to ensure that the Individual is actually who they say they are. The GHP Employee shall request the following types of information from the Individual (e.g. last four digits of the Social Security number, date of birth (month and day only)). If a GHP Employee is unable to conclusively verify the identity of the Individual, NO PHI will be discussed on the telephone. In no case may PHI be discussed on a cell phone.

E. Office Safeguards

Only GHP Employees with appropriate clearance will be provided access to PHI. Only IT Personnel will perform technical system maintenance on any computer hardware or software containing PHI. Any outside entity performing operating and maintenance services on computer hardware or software containing PHI will be monitored by IT Personnel or other employees of the Group Health Plan. Personnel clearance and security procedures will be maintained and employed by Corteva Agriscience Security, and all personnel will be trained in system security. Any maintenance will be documented in writing and maintained by IT Personnel or other employees of the Group Health Plan.

After hours. The offices of GHP Employees shall be locked and secured during non-business hours.

Conference Rooms. Users of conference rooms will ensure that PHI and other proprietary information is secure throughout the duration of the meeting and that all information is removed from the room at the close of the meeting.

Collection Bins. Receptacles (e.g. PIP boxes) used for collection and/or storage of PHI and proprietary information will be locked and immobile.

Guests. No guest shall be permitted within the Health Management Group office unless escorted by an GHP Employee, unless that guest is a Corteva Agriscience employee and is entering the Health Management Group office to meet with an GHP Employee or other human resource employee to discuss benefit or employment matters.

Termination. When a GHP Employee who has access to PHI is terminated, that access to PHI shall immediately be terminated. If that terminated employee has a key or access card, it will be immediately retrieved from the terminated employee.

F. Breach Notification

In accordance with requirements under HITECH, the HIPAA Privacy Official shall investigate any reported breach of PHI to determine if any notifications or other actions are required under HITECH or the Corteva Agriscience Corporate Procedure for Notification of a Security Breach of Personal Information (the “Corteva Agriscience Breach Procedures”). Procedures for analyzing a breach are included in the Corteva Agriscience Breach Procedures. The HIPAA Privacy Official shall maintain a log of breaches.
required to be reported to HHS and shall report such breaches to HHS annually (if not previously reported) as required by HHS IV.

IV. Health Plan Privacy Administration

A. HIPAA Privacy Official

A HIPAA Privacy Official shall be appointed by Director, U.S. Region, with responsibility for overseeing compliance with HIPAA, HITECH and this Policy. Effective June 1, 2019, the HIPAA Privacy Official for the Corteva Agriscience Health Plans is Kai Cole. The HIPAA Privacy Official will either perform the following, or designate a GHP Employee to perform the following:

1. develop, implement, and update Health Plan privacy policies and procedures, including policies and procedures as they relate to security of electronic information and breach notification,

2. ensure appropriate privacy training for GHP Employees,

3. investigate and respond to Individuals’ complaints regarding impermissible uses or disclosures of PHI and related policy violations,

4. provide Individuals with Notice and information regarding Health Plan policies and procedures related to PHI,

5. maintain documentation of policies, notices, complaints, and related activities consistent with the record-keeping procedures in this Section, and

6. oversee relationships with business associates and enter into business associate contracts on behalf of the Health Plans.

B. Designating Group Health Plan Employees

The HIPAA Privacy Official will be responsible for choosing which employees will be designated as GHP Employees and will be responsible for informing such employees which uses and disclosures of PHI are permissible with respect to that GHP Employee’s Health Plan duties and responsibilities. No employees, other than GHP Employees should have access, accept receipt, record or transmit PHI, other than PHI that relates directly to that employee as an Individual or as otherwise specifically permitted by this Policy. For a listing of designated Group Health Plan employees, see Exhibit A.

C. Employee Training

All new GHP Employees must be trained within a reasonable time after such employee begins working as a GHP Employee. The level of training will depend upon the GHP Employee’s
access to PHI. Such training will cover safeguarding PHI, permissible uses and disclosures of PHI, Individuals’ rights with respect to PHI, applicable document retention, and disciplinary action for violations of applicable policies and procedures. Training will include compliance with security requirements for ePHI (electronic PHI) and will include specific information on identity of other GHP Employees with whom PHI may be shared.

The HIPAA Privacy Official will ensure that additional training is provided if one or more of these privacy policies changes in a material way. Such additional training will be delivered within a reasonable time after the change becomes effective.

The HIPAA Privacy Official or his designee must maintain a record of all such training consistent with the record-keeping procedures in this Section.

D. Remedies for Violations of Protected Health Information Privacy Policies and Procedures

Any complaints regarding these Policies and Procedures or other report of impermissible uses or disclosures of PHI shall be forwarded to the HIPAA Privacy Official, or his designee. Such complaints will be promptly investigated. Any GHP Employee who violates a privacy policy or procedure will be subject to disciplinary action up to and including discharge.

Mitigation - A GHP Employee is required to mitigate harm resulting from an impermissible use or disclosure. If a GHP Employee is aware of an impermissible use or disclosure the GHP Employee will report the impermissible use or disclosure to the HIPAA Privacy Official immediately and shall cease from performing the use or practice which resulted in an impermissible use or disclosure. If the GHP Employee fails to: 1) report the impermissible use or disclosure; and/or 2) ceases to take any action to mitigate the harm of such an impermissible use or disclosure, disciplinary action also will apply to that employee.

Intimidation or Retaliation – A GHP Employee who intimidates or retaliates against an Individual for exercising his HIPAA rights, shall be subject to disciplinary action. In addition, disciplinary action shall be taken against a GHP Employee who intimidates or retaliates against an Individual who files a complaint with the Secretary of Health and Human Services, testifies or assists in the participation of an investigation or compliance review, proceeding or hearing, or opposes any act or practice which he or she reasonably believes is unlawful under HIPAA. If such opposition is taken, it must be taken in a reasonable manner and will not involve the disclosure of PHI in violation of HIPAA.

The HIPAA Privacy Official, or his designee must document the investigation and disciplinary action taken and must maintain such documentation consistent with the record-keeping procedures in Policy Section IV.G.
E. Reporting Policy Violations

Each GHP Employee must promptly report violations of these Policies and Procedures to the HIPAA Privacy Official. In addition, other employees shall be informed through the Privacy Notice how to report a violation to the HIPAA Privacy Official. Each such report will be subject to the investigation and remedy provisions described in Policy Section IV.D.

F. Written Policies and Procedures

These comprehensive privacy policies and procedures shall be maintained at all times by the Health Plan. The HIPAA Privacy Official shall be responsible for amending these policies and procedures. The HIPAA Privacy Official shall ensure that all amendments are in writing and communicated to GHP Employees and other necessary parties. The HIPAA Privacy Official shall enforce and ensure that all GHP Employees adhere to these written policies and procedures. If an unforeseen circumstance requires a deviation from these written policies and procedures, the HIPAA Privacy Official shall decide whether or not to grant an exception from complying with the requirements herein.

G. Record-keeping

The HIPAA Privacy Official or his designee must retain the following records either in paper or electronic form for six years from the date of creation or the date when it was last in effect, whichever is later. The following records must be retained: Privacy Policies and Procedures, Authorizations and related revocations, training records, designation of HIPAA Privacy Official, complaints and related investigations and sanctions, requests for restrictions on uses and disclosures, and uses and disclosures of PHI subject to an Accounting. In addition to the above requirements, record keeping and retention shall be followed in accordance with Corteva Agriscience CRIM guidelines.

1. Documenting Certain Uses and Disclosures

For purposes of providing an Individual an Accounting of his PHI, the Health Plan must record each instance in which the GHP Employee uses or discloses PHI unless such use or disclosure is made -

(a) for purposes of Payment or Health Care Operations and stored other than in an electronic health record;

(b) to the Individual about his own PHI;

(c) for national security or intelligence purposes;

(d) to correctional institutions or law enforcement officer; or

(e) prior to April 14, 2003.
2. The record for each use and disclosure for which a record must be maintained must include the date, name of the recipient (and address if known), description of information disclosed, and purpose for the disclosure (or a copy of the request for disclosure or the Individual’s Authorization). Such record will be retained in the Individual’s Health Plan file.

3. **Authorizations, revocations, and other Individual requests**

The HIPAA Privacy Official or his designee must maintain a copy of each Individual authorization, revocation of authorization, request for restriction on use, an Individual’s request for access to PHI, an Individual’s request to amend PHI, or an Individual’s request for an Accounting. Such record will be retained in the Individual’s Health Plan file.

4. **Training Records**

Training records must include the names of those attending, the date when and location where training was provided, and a copy of the training materials. Such record will be retained electronically or in a locked file cabinet.

5. **Complaints and Remedial Action**

Complaint files must document each reported complaint and known policy violation, related investigation and findings, and the remedial action taken to address these complaints. If such complaint is made by an Individual, a copy of the complaint and investigation shall be maintained in the Individual’s Health Plan file. If a complaint is made by someone other than an Individual, then the complaint will be maintained in a locked file cabinet.

6. **Privacy Policy**

Copies of all HIPAA Privacy Policy and Procedures, including a security risk analysis of ePHI as required by the Security Rule, shall be maintained by the HIPAA Privacy Official.

7. **Breach Policy and Notifications**

Copies of the Corteva Agriscience Corporate Procedure for Notification of a Security Breach of Personal Information, the log with information provided to HHS of each breach, and copies of notifications provided of any breach shall be retained by the HIPAA Privacy Official for a minimum of six years.

8. **Privacy Notices**

All versions of the Privacy Notice and the dates such version was in use must be retained by Corteva Agriscience Legal. In addition, a record of the dates and the means such Privacy Notice was distributed will be maintained in order to ensure that the notice is distributed no less than once every three years.
9. **Business Associate Contracts**

The HIPAA Privacy Official shall maintain copies of all final, executed business associate contracts or ensure copies are kept with Sourcing in a permanent record following termination of a relationship with a business associate.

H. **Release of PHI to a Business Associate**

The Health Plan may subcontract out some or all of the Health Plan’s administration to a Business Associate. The HIPAA Privacy Official will ensure that any disclosure of PHI to Business Associates who are engaged to create or receive PHI on behalf of the Health Plan, shall comply with HIPAA. Such compliance will involve ensuring that the Health Plan obtains satisfactory assurance that each such Business Associate will safeguard the PHI. In general, satisfactory assurance will be obtained by executing a contract with the Business Associate that:

1. establishes the permitted and required uses and disclosures of PHI by that Business Associate;

2. provides that the Business Associate must not use or further disclose the information other than as permitted by the contract or required by law;

3. requires the Business Associate to safeguard the information to prevent impermissible uses or disclosures;

4. requires the Business Associate to report breaches of the contract’s privacy provisions to the HIPAA Privacy Official, or his designee;

5. requires the Business Associate to ensure its agents, employees, and subcontractors to whom it discloses PHI agree to the same restrictions and conditions as apply to the Business Associate;

6. requires the Business Associate to make available PHI for Individuals’ access as described in Policy Section V.B;

7. requires the Business Associate to make available PHI for Individuals to amend and to incorporate such amendments if required pursuant to Policy Section V.E;

8. requires the Business Associate to make available the information necessary to provide an accounting as required under Policy Section V.F, including use and disclosures for treatment, payment and health care operations;

9. requires the Business Associate to make its internal practices, books, and records related to use and disclosure of PHI in connection with the Health Plan available to the Secretary of Health and Human Services for compliance reviews;
10. requires the Business Associate to return or destroy all PHI connected with Health Plan participants and retain no copies, if feasible, upon termination of the contract. If return or destruction is not possible, the contract must require the Business Associate to extend the protections of the contract to the information and limit further uses and disclosures to the purposes that make return or destruction infeasible;

11. requires the Business Associate to comply with the Security Rule and HITECH security requirements for ePHI, and to identify a HIPAA Privacy Official with responsibility for ensuring compliance with HIPAA and HITECH; and

12. requires the Business Associate to report any breach of PHI promptly to the HIPAA Privacy Official and take all steps necessary to comply with the breach notification rules of HITECH.

The contract must also authorize termination by the Health Plan if it determines that the Business Associate has breached a material contract privacy provision.

If any GHP Employee becomes aware of a breach of the contractual privacy provisions by a Business Associate, the GHP Employee must report that breach to the HIPAA Privacy Official. If the breach is material and the Business Associate does not cure the breach, the Health Plan must terminate the contract with the Business Associate if possible and, if termination is not possible, report the breach to the Secretary of Health and Human Services.

V. **Individuals’ Rights Regarding Protected Health Information**

An Individual has a number of rights under the HIPAA Privacy Rule, including the right to receive a privacy notice containing the Health Plan’s legal duties regarding uses and disclosures of PHI, the right to access and amend PHI in the Designated Record Set, the right to request restrictions on uses and disclosures of PHI, and the right to an accounting of certain uses and disclosures of PHI. Under no circumstances will Health Plan enrollment or benefit payment be conditioned on an Individual’s waiver of his rights to file a complaint with the Secretary of Health and Human Services. All forms utilized by Individuals to exercise their rights are found in Exhibit B.

A. **Privacy Notice**

Corteva Agriscience, on behalf of the Health Plan, must notify Individuals covered by the Health Plan of the uses and disclosures of PHI that will be made by the Health Plan, the Individual’s rights and the Health Plan’s legal duties with respect to PHI. Such notice must be provided to each covered employee at the time of enrollment for new enrollees, and must be posted on the Corteva Agriscience website at https://hr.Corteva Agriscience.com/en/Pages/Corteva Agriscience-Protected-Health-Information-Forms.aspx. A copy of the current notice is in Exhibit C.
The notice must be revised whenever there is a material change to the uses and disclosures, Individuals’ rights, the Health Plans’ duties, or other privacy practices stated in the notice. Revised notices must be distributed to covered employees and posted at https://hr.CortevaAgriscience.com/en/Pages/CortevaAgriscience-Protected-Health-Information-Forms.aspx within 60 days of the material change. If a new HIPAA Privacy Official is appointed, all Individuals will receive written notice and the information will be posted on the HIPAA website noted above. A Privacy Notice may not be combined with an Authorization.

No less frequently than once every three years, the Group Health Plan must notify covered employees of the right of Individuals to obtain a copy of the notice and how to do so.

B. Access to Protected Health Information

The Health Plan must permit an Individual or Personal Representative to inspect and obtain a copy of PHI within a Designated Record Set, except for information compiled in preparation for legal or an administrative proceeding. A request for access must be made in writing and submitted to the HIPAA Privacy Official, or his designee.

A Designated Record Set will include an Individual’s enrollment records, contribution amounts paid by Corteva Agriscience or the Individual for his coverage under the Health Plan, Explanation of Benefits or other claim payment records, or any medical management records. A record will consist of any item, collection, or grouping of information that contains PHI and is either maintained, collected, used or disseminated by or for the Health Plan. A Designated Record Set does not include psychotherapy notes, information compiled in reasonable anticipation of, or for use in a legal or administrative proceeding; or information subject to specific provisions of the Clinical Laboratory Improvements Amendments of 1988.

Timing of Response and Providing Access. Upon receipt of the written request, the HIPAA Privacy Official, or his designee must provide the requested access, provide a written denial notice, or provide written notice that an extension of time is needed to respond to the request. HIPAA requires this process to take no longer than 30 days for internal Corteva Agriscience GHP records, or no longer than 60 days for external records maintained by carriers.

Information not Maintained by the Health Plan. If the information is maintained by a Business Associate for the Health Plan, the HIPAA Privacy Official, or his designee must instruct the Business Associate to make available the PHI so that the requested access can be provided within these time frames. If the Individual requested access to PHI not maintained by or for the Health Plan, but the HIPAA Privacy Official, or his designee knows where the information is maintained, the Privacy Official must inform the Individual where to direct his request.

Request for an Extension. If access is to be granted but cannot be granted within 30 days of the request, the Health Plan will have up to 30 additional days to provide access as long as the Individual is notified in writing of the reason for the delay and the additional time needed to comply before the expiration of the first 30-day period.

Denying the Request. The Health Plan will deny the Individual’s request to inspect or obtain a copy of PHI if any of the following apply:
1. The PHI was obtained from someone other than a health care carrier under a promise of confidentiality and the requested access, if granted, likely would reveal the source of information;

2. A licensed health care professional has determined that the requested access, if granted, likely would endanger the life or physical safety of the Individual or another person;

3. The PHI makes reference to another person (other than a health care carrier) and a licensed health care professional has determined that the requested access, if granted, likely would cause substantial harm to that referenced person; or

4. The request is made by a Personal Representative and a licensed health care professional has determined that the requested access, if granted, likely would cause substantial harm to the Individual or another person.

If access is denied for reason 2, 3, or 4 above, the Individual has the right to have the denial reviewed by a licensed health care professional designated by the Health Plan to act as a review officer. This review officer cannot be someone who participated in the original decision to deny access.

Contents of a Denial. Each denial must be provided in writing and include the following:

1. A statement of the reason for denial;

2. The procedure for requesting review of the denial, if applicable; and

3. The procedure for filing a complaint with the HIPAA Privacy Official or the Secretary of Health and Human Services.

If requested, the review must be promptly given and, if access is again denied on review, written notice must be given promptly to the Individual.

Record Retention. The Health Plan must document the actual request, current HIPAA Privacy Official or designee responsible for receiving and processing requests for access, and the specific PHI subject to the access. Such documentation must be maintained in accordance with the record-keeping procedures in Policy Section IV.G.

C. Request for Restriction on Uses and Disclosures

An Individual may request that the Health Plan restrict in a specified way uses and disclosures of PHI for Payment and Health Care Operations. Such a request must be made in writing and submitted to the HIPAA Privacy Official or his designee.
Effect of Restriction. If the Health Plan agrees to the requested restriction, GHP Employees will not thereafter use or disclose PHI for Payment or Health Care Operations inconsistently with the restriction unless the restriction agreement is terminated, or such inconsistent use or disclosure is necessary to provide emergency treatment. If the GHP Employee discloses the restricted PHI to a health care carrier in such emergency, the GHP Employee must request that the carrier not further disclose it. This restriction will not apply to uses and disclosures conducted prior to the Health Plan’s agreement to the restriction.

The Health Plan will terminate a restriction agreement by informing the Individual of such termination.

Record Retention. All restriction requests, agreements, and terminations must be documented, and such documentation must be retained in accordance with the record-keeping procedures in Policy Section IV.G.

D. Confidential Communication

An Individual may request alternative means of receiving communication of his PHI and the Health Plan must accommodate each reasonable request. Such a request must be made in writing, include the alternative communication means and a statement that disclosure otherwise could endanger the Individual and be submitted to the HIPAA Privacy Official his designee.

E. Amendment of Protected Health Information

An Individual has a right to request that the Health Plan amend his PHI within a Designated Record Set. Such a request must be made in writing, submitted to the HIPAA Privacy Official and must provide a reason to support such amendment.

Timing of Response. Within 60 days of receiving the request, the HIPAA Privacy Official or his designee must either amend the information as requested, provide a written denial notice, or provide written notice that an extension of time is needed to respond to the request. If an amendment is to be granted, but an extension of time is needed, the Health Plan will have up to 30 additional days to amend the PHI as long as the Individual is notified in writing of the reason for the delay and the additional time needed to comply before the expiration of the first 60-day period.

Granting the Request. If the request is granted, the HIPAA Privacy Official must (a) amend the information, (b) inform the Individual of the amendment, and notify both persons identified by the Individual as needing notice of the amendment and Business Associates who may already have relied or may rely in the future on such information.

Denying the Request. The Individual’s request to amend his PHI will be denied if the HIPAA Privacy Official determines that –
1. the information was not created by the Health Plan (unless the creator no longer is available to amend it and the HIPAA Privacy Official otherwise determines that it should be amended under this policy);

2. it is not part of the Designated Record Set;

3. it is not accessible to the Individual under Policy Section V.B; or

4. the information is complete and accurate.

If the request is denied, the HIPAA Privacy Official must provide the basis for the denial in writing. The written denial also must inform the Individual of his right to (a) submit a written statement to the HIPAA Privacy Official disagreeing with the denial, and the procedure for such submission (b) or if he chooses not to submit a disagreement, his right to ask for his request and the denial of such request accompany any future disclosures of the subject PHI, or (c) the procedure for filing a complaint with HIPAA Privacy Official or Secretary of Health and Human Services. The HIPAA Privacy Official will rebut statements of disagreement in writing to the Individual, if rebuttal is applicable. Any such request for amendment, statement of disagreement, and rebuttal must be included with future disclosures of the subject PHI.

Notice of Amendment from Another Entity. If the Health Plan receives notice of an amendment from a health care carrier or other Covered Entity under the Privacy Rule, the HIPAA Privacy Official must amend the subject PHI.

Record Retention. The Health Plan must document the current HIPAA Privacy Official responsible for receiving and processing requests for amendments and retain such documentation in accordance with the record-keeping procedures in Policy Section IV.G.

F. Accounting

An Individual has the right to request an accounting of certain Health Plan disclosures of PHI in the six-year period prior to the request. Each request for an accounting must be submitted in writing to the HIPAA Privacy Official and include for each disclosure, the date, name of recipient (and address, if known), description of information disclosed and purpose for the disclosure, and a brief statement informing the Individual of the basis of the disclosure. (See Exhibit B, HIPAA Forms).

An Individual does not have the right to an accounting of Health Plan disclosures made:

1. to carry out Treatment, Payment or Health Care Operations, except that an Individual is entitled to an Accounting of uses of ePHI acquired on or after January 1, 2011, and disclosed in the three years preceding the request;

2. to the Individual about his own PHI;

3. incident to a use or disclosure permitted by the Privacy Rule;
4. pursuant to an Authorization;

5. for national security or intelligence purposes;

6. to correctional institutions or law enforcement officer; or

7. prior to April 14, 2003.

For a disclosure under item 1 above, the HIPAA Privacy Official may provide ePHI held by a Business Associate directly to the Individual or may provide the Individual with contact information for all Business Associate holding ePHI for the Individual.

**Multiple Disclosures** - If the Health Plan has made multiple disclosures of PHI to the same person or entity for a single purpose, then the accounting may provide the following:

1. the elements of an accounting (mentioned above), but only for the first disclosure;

2. the frequency, periodicity, or number of the disclosures made during the accounting period; and

3. the date of the last such disclosure during the accounting period.

The Health Plan will provide one such accounting in a 12-month period without charge and will charge a reasonable fee for subsequent accountings requested in the same 12-month period. The Individual’s right to an accounting will be subject to certain public health and law enforcement related restrictions provided under the Privacy Rule.

**Suspension of an Individual’s right to an accounting** - The Health Plan must temporarily suspend an Individual’s right to receive an accounting of disclosures to a health oversight agency or law enforcement official (See Policy Sections II.D and I.F.3) if such agency or official provides the HIPAA Privacy Official with a written statement, then that statement must say that such an accounting to the Individual would likely impede the agency’s activities and specify the time for the required suspension.

If the statement is made orally, the Health Plan must do the following:

1. document the statement, including the identity of the agency or official making the statement;

2. temporarily suspend the Individual’s right to an accounting of disclosures subject to the statement; and

3. limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.
Timing of Response. Within 60 days of receiving the request, the HIPAA Privacy Official must either provide the Individual with an accounting, provide a written denial notice, or provide written notice that an extension of time is needed to respond to the request. If an amendment is to be granted, but an extension of time is needed, the Heath Plan will have up to 30 additional days to amend the PHI as long as the Individual is notified in writing of the reason for the delay and the additional time needed to comply before the expiration of the first 60-day period.

Record Retention. The Health Plan must document the current HIPAA Privacy Official who is responsible for receiving and processing requests for an accounting, the information subject to the accounting, and the written accounting provided to the Individual. Such documentation must be maintained in accordance with the record-keeping procedures in Policy Section IV.G.

G. Complaints

An Individual who lodges a complaint about these policies and procedures and compliance with the Privacy Rule, will complain to the HIPAA Privacy Official. The HIPAA Privacy Official must investigate all such complaints and will provide written response to submitted complaints in writing (other than anonymously) by an Individual. Each complaint must be handled in accordance with Policy Section IV.D. The HIPAA Privacy Official must retain documentation of each such complaint, investigation, response, and disposition in accordance with the record-keeping procedures in Policy Section IV.G.

H. Personal Representatives

An Individual’s Personal Representative (appointed by operation of law; see definition) enjoys the same rights and responsibilities under these privacy policies as the Individual. If under state law, a person has the authority to act on behalf of an Individual who is an adult or emancipated minor in making health care decisions, then that person is the Individual’s Personal Representative. If under state law, a person has the authority to act on behalf of an Individual who is an un-emancipated minor in making health care decisions, then that person is the Individual’s Personal Representative with limited exceptions.

When a Parent is not a Personal Representative. A parent or guardian will not be treated as the Personal Representative of an un-emancipated minor under the following circumstances:

1. The minor has the legal right to consent to health care without the consent of a parent or guardian and the minor obtains the consent of the court or another person authorized by law to provide the consent;

2. The minor has consented to such health care and no other consent is required by law (even if consent of another has been obtained) and the minor has not requested that such person be treated as his/her Personal Representative;
3. The minor’s parent or guardian has consented to confidentiality with the minor’s medical carrier; or

4. If the GHP Employee believes that the Personal Representative has subjected or may subject the Individual to domestic violence, abuse, or neglect or otherwise endanger the Individual, the Personal Representative will not be treated as the Individual.

GHP Employees will take reasonable steps to ensure the status of each Personal Representative. For example, guardians and conservators should produce documents verifying such appointments. A Personal Representative will produce a birth certificate, adoption papers, or other legal document which states he/she is the legal guardian or parent of the Individual.
EXHIBIT A:

GROUP HEALTH PLAN EMPLOYEES

Employees of the Group Health Plan (GHP) shall have access to Protected Health Information only in connection with performance of the administrative functions that the Plan Sponsor performs for the Plan. Effective June 1, 2019, the Group Health Plan Employees that shall have access to such Protected Health Information include:

- Health Care Policy Team (Tijana Omerovich, Jennifer Sloan)
- Health Care Administration Team (Sue Arling-Hoover, Pat Carter, Elizabeth Krieg, Michele Riley, Maria Tillinghast and Megan Tomlin)
- HIPAA Privacy Official (Kai Cole)
- Benefit Appeals Committee

Select Members of the following group:
- Legal, Employee Benefits (Lori Knauer)
- Healthcare Actuarial (Patty Yang)
EXHIBIT B: HIPAA

FORMS

• All HIPAA Forms are available at:
  https://agcompany.sharepoint.com/sites/hr/en/Pages/DuPont-Protected-
  Health-Information-Forms.aspx

• **Authorization Form for the Use and Disclosure of Protected Health Information**
The Authorization Form for the Use and Disclosure of Protected Health Information (PHI) should be
used when you wish to allow your PHI to be disclosed to another person or entity.

• **Revocation of Authorization to Release PHI**
The Revocation of Authorization to Release PHI Form should be used when you want to revoke prior
authorization to disclose your PHI to another person or entity.

• **Request for Restriction on Use & Disclosure and/or Confidential Communication of PHI**
The Request for Restriction on Use & Disclosure and/or Confidential Communications of PHI should be
used when you would like to restrict or limit the PHI we disclose about you and/or ask us to communicate your PHI in a certain way or location if the current manner would endanger you.

• **Request for Amendment/Correction of PHI**
The Request for Amendment/Correction of PHI Form should be used if you believe that your PHI is
incorrect or that an important part of it is missing.

• **Request for Accounting of Disclosure of PHI**
The Request for Accounting of Disclosures of PHI Form should be used to request a list of certain
disclosures of PHI we have made about you. Please note that the time period of your request may not
be longer than 6 years and may not include dates before April 14, 2003.

• **Request for Inspection/Copy of PHI**
The Request for Inspection/Copy of PHI may be used to inspect and obtain a copy of the PHI that the
Health Plans maintain about you. Request for Restriction on Use & Disclosure and/or Confidential

• **Complaint Form**
The Complaint Form should be used if you believe your privacy rights have been violated. Complaints
may be filed with the HIPAA Privacy Official for the Corteva Agriscience Health Plans or with the
Secretary of the Department of Health and Human Services.

• **Confidential FAX Coversheet**
The Confidential Fax Form has been provided for your convenience when faxing information
containing PHI.

• **Notice of Misdirected FAX**
In the event that you discover your fax containing PHI has been sent to the wrong recipient, use the
Misdirected Fax Form may assist in protecting your information from further circulation.
EXHIBIT C:

PRIVACY NOTICE

HIPAA Notice of Privacy Practices for Protected Health Information

Corteva HIPAA Notice.pdf

HIPAA Privacy Notice Final 2019