Jeffrey M. Wright, M.D.
Lisa V. Suffian, M.D.
Gary M. Goodman, M.D.
Alexia Munter, FNP-BC

456 N. New Ballas Road, Suite 129
St. Louis, Missouri 63141
(314)569-1881
FAX: (314)569-3277

Notice of Privacy Practices

This Notice of Privacy Practices describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.

If you have any questions about this Notice, please contact our Privacy Officer, Barbara Faupel

***Revisions 2023

This Notice of Privacy Practices describes how Allergy Consultants may use and disclose your protected health information to carry out treatment, payment, or healthcare operations and for other purposes that are permitted or required by law. It also describes your rights to access and control your protected health information. "Protected health information" or "PHI" is information about you, including demographic information, that may identify you and that relates to your past, present, or future physical or mental health or condition and related healthcare services.

We are required to abide by the terms of this Notice of Privacy Practices. We may change the terms of our notice, at any time. The new notice will be effective for all protected health information that we maintain at that time. We will provide you with any revised Notice of Privacy Practices by calling the office and requesting that a revised copy be sent to you in the mail or asking for one at the time of your next appointment.

1. USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION FOR TREATMENT, PAYMENT, AND HEALTHCARE OPERATIONS

Your PHI may be used and disclosed for treatment, payment, and healthcare operations by your physician, our office staff, and others outside of our office that are involved in your care and treatment for the purpose of providing healthcare services to you. Your PHI also may be used and disclosed to pay your healthcare bills and to support the operation of the physician's practice.

Following are examples of the types of uses and disclosures of your protected healthcare information that the physician's office is permitted to make. These examples are not meant to be exhaustive, but to describe the types of uses and disclosures that may be made by our office.

Treatment: We will use and disclose your protected health information to provide, coordinate, or manage your healthcare and any related services. This includes the coordination or management of your healthcare with a third party that has already obtained your permission to have access to your protected health information. For example, we would disclose your protected health information, as necessary, to a home healthcare agency that provides care to you or to whom you have been referred to ensure that the physician has the necessary information to diagnose or treat you.

In addition, we may disclose your protected health information from time to time to another physician or healthcare provider (e.g., a specialist or laboratory) who, at the request of your physician, becomes involved in your care by providing assistance with your healthcare diagnosis or treatment to your physician.

Payment: Your protected health information will be used, as needed, to obtain payment for your healthcare services. This may include certain activities that your health insurance plan may undertake before it approves or pays for the healthcare services we recommend for you such as making a determination of eligibility or coverage for insurance benefits; reviewing services provided to you for medical necessity; and undertaking utilization review activities. For example, obtaining approval for a hospital stay may require that your relevant protected health information be disclosed to the health plan to obtain approval for the hospital admission.

Healthcare Operations: We may use or disclose, as needed, your protected health information in order to support the operations of your physician's practice. These operations include, but are not limited to, quality assessment activities, employee review activities, training of medical students, licensing, marketing, and fundraising activities, and conducting or arranging for other business activities.

For example, we may disclose your protected health information to medical school students that see patients at our office. We also may call you by name in the waiting room when your physician is ready to see you. We may use or disclose your protected health information, as necessary, to contact you to remind you of your appointment. (Please see Section 6 if you wish to opt out of being called by name or being contacted for appointments.)

We will share your protected health information with third party "business associates" that perform various services (e.g., billing, legal services, or transcription services) for the practice. Whenever an arrangement between our office and a business associate involves the use or disclosure of your PHI, we will have a written contract that contains terms that will protect the privacy of your PHI in the hand of our business associates.

We may use or disclose your protected health information, as necessary, to provide you with information about treatment alternatives or other health-related benefits and services that may be of interest to you. We also may use and disclose your protected health information for certain marketing activities. You may contact our Privacy Officer to request that these materials not be sent to you.

2. USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION BASED UPON YOUR WRITTEN AUTHORIZATION

Other uses and disclosures of your protected health information will be made only with your written authorization, unless otherwise permitted or required by law as described below. You may revoke this authorization, at any time, in writing, except to the extent that your physician or the physician's practice has taken an action in reliance on the use or disclosure indicated in the authorization.

*****Childhood Immunizations** We may disclose immunizations to schools that require proof of immunizations prior to admitting the student so long as the physicians have and document the patient or patient's legal representative's "written agreement" to the disclosure.

3. OTHER PERMITTED AND REQUIRED USES AND DISCLOSURES THAT MAY BE MADE WITH YOUR CONSENT, AUTHORIZATION, OR OPPORTUNITY TO OBJECT

We may use and disclose your PHI in the following instances. You have the opportunity to agree or object to the use or disclosure of all or part of your PHI. If you are not present or able to agree to or object to the use or disclosure of the protected health information, then your physician may, using his or her professional judgment, determine whether the disclosure is in your best interest. In this case, only the protected health information that is relevant to your healthcare will be disclosed.

Others Involved in Your Healthcare: Unless you object, we may disclose to a member of your family, a relative, a close friend, or any other person you identify, your protected health information that directly relates to that person's involvement in your healthcare. If you are unable to agree or object to such a disclosure, we may disclose such information as necessary if we determine that it is in your best interest based on our professional judgment. We may use or disclose protected health information to notify or assist in notifying a family member, personal representative, or any other person that is responsible for your care of your location, general condition, or death. Finally, we may use or disclose your protected health information to an authorized public or private entity to assist in disaster relief efforts and to coordinate uses and disclosures to family or other individuals involved in your healthcare.

*****Decedents:** We recognize that a deceased patients PHI may be relevant to a family member's health care. There are two ways for a surviving family member to obtain the protected health information of a deceased relative.

(i) Disclosures of protected health information for treatment purposes—even the treatment of another individual—do not require an authorization; thus, a covered entity may disclose a decedent's protected health information, without authorization, to the health care provider who is treating the surviving relative.

(ii) A covered entity must treat a deceased individual's legally authorized executor or administrator, or a person who is otherwise legally authorized to act on the behalf of the deceased individual or his estate, as a personal representative with respect to PHI relevant to such representation.

Therefore, if it is within the scope of such personal representative's authority under other law, the Rule permits the personal representative to obtain the information or provide the appropriate authorization for its disclosure within a fifty (50) year time frame post death.

Emergencies: We may use or disclose your protected health information in an emergency treatment situation. If this happens, your physician will try to obtain your consent as soon as reasonably practicable after the delivery of treatment. If your physician or another physician in the practice is required by law to treat you and the physician has attempted to obtain your consent but is unable to obtain your consent, he or she may still use or disclose your protected health information to treat you.

Communication Barriers: We may use and disclose your protected health information if your physician or another physician in the practice attempts to obtain consent from you but is unable to do so due to substantial communication barriers and the physician determines, using professional judgment, that you intend to consent to use or disclosure under the circumstances.

4. OTHER PERMITTED AND REQUIRED USES AND DISCLOSURES THAT MAY BE MADE WITHOUT YOUR CONSENT, AUTHORIZATION, OR OPPORTUNITY TO OBJECT

We may use or disclose your protected health information in the following situations without your consent or authorization. These situations include:

Required By Law: We may use or disclose your protected health information to the extent that the use or disclosure is required by law. The use or disclosure will be made in compliance with the law and will be limited to the relevant requirements of the law. You will be notified, as required by law, of any such uses or disclosures.

Public Health: We may disclose your protected health information for public health activities and purposes to a public health authority that is permitted by law to collect or receive the information. The disclosure will be made for the purpose of controlling disease, injury, or disability. We may also disclose your protected health information, if directed by the public health authority, to a foreign government agency that is collaborating with the public health authority.

Communicable Diseases: We may disclose your protected health information, if authorized by law, to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading the disease or condition.

Health Oversight: We may disclose protected health information to a health oversight agency for activities authorized by law, such as audits, investigations, and inspections. Oversight agencies seeking this information include government agencies that oversee the healthcare system, government benefit programs, other government regulatory programs, and civil rights laws.

Abuse or Neglect: We may disclose your protected health information to a public health authority that is authorized by law to receive reports of child abuse or neglect. In addition, we may disclose your protected health information if we believe that you have been a victim of abuse,

neglect, or domestic violence to the governmental entity or agency authorized to receive such information. In this case, the disclosure will be made consistent with the requirements of applicable federal and state laws.

Food and Drug Administration: We may disclose your protected health information to a person or company required by the Food and Drug Administration to report adverse events, product defects or problems, biologic product deviations, track products, to enable product recalls, to make repairs or replacements, or to conduct post marketing surveillance, as required.

Legal Proceedings: We may disclose protected health information in the course of any judicial or administrative proceeding, in response to an order of a court or administrative tribunal (to the extent such disclosure is expressly authorized), in certain conditions in response to a subpoena, discovery request, or other lawful process.

Law Enforcement: We may also disclose protected health information, so long as applicable legal requirements are met, for law enforcement purposes. These law enforcement purposes include (1) legal processes and as otherwise required by law, (2) limited information requests for identification and location purposes, (3) information pertaining to victims of a crime, (4) suspicion that death has occurred as a result of criminal conduct, (5) in the event that a crime occurs on the premises of the practice, and (6) medical emergency (not on the practice's premises) and it is likely that a crime has occurred.

Coroners, Funeral Directors, and Organ Donation: We may disclose protected health information to a coroner or medical examiner for identification purposes, determining cause of death or for the coroner or medical examiner to perform other duties authorized by law. We also may disclose protected health information to a funeral director, as authorized by law, in order to permit the funeral director to carry out their duties. We may disclose such information in reasonable anticipation of death. Protected health information may be used and disclosed for cadaveric organ, eye, or tissue donation purposes.

Research: We may disclose your protected health information to researchers when their research has been approved by an institutional review board that has reviewed the research proposal and established protocols to ensure the privacy of your protected health information.

Criminal Activity: Consistent with applicable federal and state laws, we may disclose your protected health information, if we believe that the 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. We may also disclose protected health information if it is necessary for law enforcement authorities to identify or apprehend an individual.

Military Activity and National Security: When the appropriate conditions apply, we may use or disclose protected health information of individuals who are Armed Forces personnel (1) for activities deemed necessary by appropriate military command authorities; (2) for the purpose of a determination by the Department of Veterans Affairs of your eligibility for benefits, or (3) to foreign military authority if you are a member of that foreign military services. We also may disclose your protected health information to authorized federal officials for conducting national security and intelligence activities, including for the provision of protective services to the President or others legally authorized.

Workers' Compensation: Your protected health information may be disclosed by us as authorized to comply with workers' compensation laws and other similar legally-established programs.

Inmates: We may use or disclose your protected health information if you are an inmate of a correctional facility and your physician created or received your protected health information in the course of providing care to you.

Required Uses and Disclosures: Under the law, we must make disclosures to you and when required by the Secretary of the Department of Health and Human Services to investigate or determine our compliance with the requirements of Title 45, Section 164.500 et. seq. of the Code of Federal Regulations.

*****5. MARKETING** HITECH Act section 13406(a) limits the health-related communications that may be considered health care operations and thus that are accepted from the definition of "Marketing" under the HIPAA Privacy Rule, to the extent that a Covered Entity has received direct or indirect payment in exchange for making the communication.

In cases where a Covered Entity would receive payment the HITECH Act requires a Covered Entity to obtain authorization prior to making the communication (applies to a Business Associate as well).

The general concept under the proposed rule that marketing means "to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service" has been maintained with some exceptions.

The proposed rule included three (3) exceptions to the general rule as follows: (1) certain health care operations ("HCOs") are excluded except where the Covered Entity receives financial remuneration for the communication such as: (a) describing a health-related product or service that is provided by the Covered Entity; (b) case management and coordination; (c) contacting persons about alternatives; and (d) similar functions (i.e. to the extent that these activities are not considered treatment); (2) communications regarding refill reminders or a biologic that is currently prescribed; and (3) removal of the language defining as marketing an arrangement between a Covered Entity and any other entity in which the Covered Entity discloses Protected Health Information to the other entity, in exchange for remuneration, to make a communication about its own product or services that encourages a purchase, because such an activity, under HITECH Act 13405(d) would now be considered a prohibited "sale" of Protected Health Information. A standalone exception for refill reminders remains in place under the HITECH Act.

6. PATIENT OPTIONS

In reminding you of appointments, our normal procedure is to call the number you have provided us and to leave a message at that number indicating the time and date of the appointment and who the appointment is with. The message will not disclose personal health information. However, if you prefer not to have such a message left, or if you would like to place certain restrictions on what type of message is left, please inform our Privacy Officer, and we will do our best to accommodate your special request.

In calling you in for your appointment, our normal procedure is to call you by name in the waiting room. If you prefer that we do not use your name to call you in for your appointment, please notify our Privacy Officer, and we will use another method to call you in to the appointment.

*****7. FUNDRAISING** Our office shall by rule provide that any fundraising communication shall, in a clear and conspicuous manner, provide an opportunity for the patient of the communications to elect not to receive any further such communication. When a patient elects not to receive any further such communication, such election shall be treated as a revocation of authorization.

*****8. RESEARCH** Currently we do not participate in research or clinical trials. At any time we have the right to amend our Notice of Privacy Practices (NPP), in doing so a revised version will be available to our patients. In addition an updated Acknowledgment of Receipt of NPP will be required from each patient.

*****9. SALE OF PHI** The HITECH Act adds a new provision to the Privacy Rule that prohibits covered entities and business associates from selling patients' PHI without authorization. The authorization must expressly state that the entity is receiving remuneration in exchange for the PHI.

The following activities are exempt from this authorization requirement:

(i) Public Health Activities
(ii) Research (covered entities and business associates may also sell PHI in LDS form for research purposes without obtaining prior authorization if the price charged reflects the cost to prepare and transmit the information.)
(iii) Treatment and Payment (Payment was not a basis for exemption originally listed in the HITECH Act, but HHS included it in the Proposed Rule and declined to impose a restriction on the amount an entity can charge for disclosing the PHI for payment purposes.)
(iv) Health Care Operations
(v) business associate Activities (Disclosures of PHI by a covered entity to a business associate or by a business associate to a third party on behalf of the covered entity are exempted, as long as any remuneration received was for payment of activities performed by the business associate pursuant to a business associate contract.)
(vi) Patient Requests (Disclosures of PHI are exempted when a patient requests access to their medical records or an accounting of disclosures. A patient's request for an accounting of disclosures was not an exception originally listed in the HITECH Act, but HHS has decided to include it in the Proposed Rule. Under the rule, HHS would also impose a restriction on the amount of remuneration the covered entity may receive for such disclosures. A covered entity would be allowed to charge patients fees that are consistent with the rules governing the specific request).

The Proposed Rule adds the following exceptions, which were not required by the language of HITECH:

(i) Required by Law (HHS added this new exception to ensure that covered entities continue to disclose PHI, where required by law, even if the covered entity receives remuneration for the disclosure).
(ii) Any Other Purpose Permitted by the Privacy Rule (HHS also added an exception for disclosures of PHI for any other purpose permitted by the Privacy Rule as long as the only remuneration received is a reasonable, cost-based fee to cover the cost of preparing and transmitting the PHI.)

*****10. COPIES OF e-PHI OR PHI** We have thirty (30) days to respond to your request for PHI, and one thirty (30) day extension, regardless of where the records are kept. When we convert to e-PHI, we must provide you with access to your EHR and/or other electronic records in electronic format if records are readily reproducible in that format. Otherwise we must provide the records in a mutually agreeable electronic format. Hard copies are permitted only when the individual rejects all readily reproducible e-formats or if our office has not yet converted to electronic format.

*****11. EMAILING e-PHI** The HITECH Act, adds a new provision that requires us to implement policies and procedures to restrict access to, protect the integrity of, and guard against unauthorized access to our patients e-PHI. Therefore it is our policy, not transmit any PHI via email or internet transmissions.

*****12. CHARGING FOR COPIES OF e-PHI OR PHI** Under HIPAA law, a covered entity may only charge an individual or the individual's personal representative a reasonable cost-based fee. Missouri sets the statutory base rate for calculating the maximum fees for copying medical records. Under the new HITECH act the cost that may be charged to an individual or the individual's personal representative could include the following:

(i) Labor for copying the protected health information requested by the individual, whether in paper or electronic form;
(ii) Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media;
(iii) Postage, when the individual has requested the copy, or the summary or explanation, be mailed;
(iv) Preparing an explanation or summary of the protected health information, if agreed to by the individual.

13. YOUR RIGHTS

Following is a statement of your rights with respect to your PHI and a brief description of how you may exercise these rights.

You have the right to inspect and copy your protected health information. This means you may inspect and obtain a copy of protected health information about you that is contained in a designated record set for as long as we maintain the protected health information. A "designated record set" contains medical and billing records and any other records that your physician and the practice use for making decisions about you.

Under federal law, however, you may not inspect or copy the following records: psychotherapy notes; information compiled in reasonable anticipation of, or use in, a civil, criminal, or administrative action or proceeding, and protected health information that is subject to law that

prohibits access to protected health information. Depending on the circumstances, a decision to deny access may be reviewable. In some circumstances, you may have a right to have this decision reviewed. Please contact our Privacy Officer if you have questions about access to your medical records.

You have the right to request a restriction of your protected health information. This means you may ask us not to use or disclose any part of your protected health information for the purposes of treatment, payment, or healthcare operations. You also may request that any part of your protected health information not be disclosed to family members or friends who may be involved in your care or for notification purposes as described in this Notice of Privacy Practices.

*******You may also ask us not to disclose information to your health plan(s) about your care, when you have paid out of pocket. Unless it is for treatment purposes, or in the rare event the disclosure is required by law. Your request must be made in writing and state the specific restriction requested and to whom you want the restriction to apply.

You have the right to request to receive confidential communications from us by alternative means or at an alternative location. We will accommodate reasonable requests. We may also condition this accommodation by asking you for information as to how payment will be handled or specification of an alternative address or other method of contact. We will not request an explanation from you as to the basis for the request. Please make this request in writing to our Privacy Officer.

You may have the right to request that your physician amend your protected health information. This means you may request an amendment of protected health information about you in a designated record set for as long as we maintain this information. In certain cases, we may deny your request for an amendment. If we deny your request for amendment, you have the right to file a statement of disagreement with us and we may prepare a rebuttal to your statement and will provide you with a copy of any such rebuttal. Please contact our Privacy Officer to determine if you have questions about amending your medical record.

You have the right to receive an accounting of certain disclosures we have made, if any, of your protected health information. This right applies to disclosures for purposes other than treatment, payment, or healthcare operations as described in this Notice of Privacy Practices. It excludes disclosures we may have made to you, to family members, or friends involved in your care, or for notification purposes. You have the right to receive specific information regarding these disclosures that occurred after April 14, 2003. You may request disclosures for a shorter time period. The right to receive this information is subject to certain exceptions, restrictions, and limitations.

You have the right to obtain a paper copy of this notice from us, upon request, even if you have agreed to accept this notice electronically.

*****14. BREACH NOTIFICATION POLICY**

A. **A covered entity** - that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, in the case of a breach of such information that is discovered by the covered entity, will notify each individual whose unsecured protected health information has been, or is reasonably believed to have been breached within the time frame discussed in section 14d.

B. **Notification of Covered Entity by Business Associate**.- A business associate of a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, following the discovery of a breach of such information, notify the covered entity of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during such breach.

C. **Breaches Treated as Discovered**.—For purposes of this section, a breach shall be treated as discovered by a covered entity or by a business associate as of the first day on which such breach is known to such entity or associate, respectively, (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of such entity or associate, respectively) or should reasonably have been known to such entity or associate (or person) to have occurred.

D. **Timeliness of Notification**.

(i) **In General**.—Subject to subsection (g), all notifications required under this section shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach by the covered entity involved (or business associate involved in the case of a notification required under subsection (b).

(ii) **Burden of Proof**.—The covered entity involved (or business associate involved in the case of a notification required under subsection (b), shall have the burden of demonstrating that all notifications were made as required under this part, including evidence demonstrating the necessity of any delay.

E. **Methods of Notice**.

(i) **Individual Notice**.—Notice required under this section to be provided to an individual, with respect to a breach, shall be provided promptly and in the following form:

(A) Written notification by first-class mail to the individual (or the next of kin of the individual if the individual is deceased) at the last known address of the individual or the next of kin, respectively, or, if specified as a preference by the individual, by electronic mail. The notification may be provided in one or more mailings as information is available.

(B) In the case in which there is insufficient, or out-of- date contact information (including a phone number, email address, or any other form of appropriate communication) that precludes direct written (or, if specified by the individual under subparagraph (A), electronic) notification to the individual, a substitute form of notice shall be provided, including, in the case that there are 10 or more individuals for which there is insufficient or out-of-date contact information, a conspicuous posting for a period determined by the Secretary on the home page of the Web site of the covered entity involved or notice in major print or broadcast media, including major media in geographic areas where the individuals affected by the breach likely reside. Such a notice in media or web posting will include a toll-free phone number where an individual can learn whether or not the individual's unsecured protected health information is possibly included in the breach.

(C) In any case deemed by the covered entity involved to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity, in addition to notice provided under subparagraph (A), may provide information to individuals by telephone or other means, as appropriate.

(ii) **Media Notice**.—Notice shall be provided to prominent media outlets serving a State or jurisdiction, following the discovery of a breach described in subsection (a), if the unsecured protected health information of more than 500 residents of such State or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach.

(iii) **Notice to Secretary**.—Notice shall be provided to the Secretary by covered entities of unsecured protected health information that has been acquired or disclosed in a breach. If the breach was with respect to 500 or more individuals than such notice must be provided immediately. If the breach was with respect to less than 500 individuals, the covered entity may maintain a log of any such breach occurring and annually submit such a log to the Secretary documenting such breaches occurring during the year involved.

(iv) **Posting on HHS Public Website**.—The Secretary shall make available to the public on the Internet website of the Department of Health and Human Services a list that identifies each covered entity involved in a breach described in subsection (a) in which the unsecured protected health information of more than 500

F. **Content of Notification**.—Regardless of the method by which notice is provided to individuals under this section, notice of a breach shall include, to the extent possible, the following:

(i) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

(ii) A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).

(iii) The steps individuals should take to protect themselves from potential harm resulting from the breach.

(iv) A brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.

(v) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll free telephone number, an e-mail address, Web site, or postal address.

G. **Delay of Notification Authorized for Law Enforcement Purposes**.—If a law enforcement official determines that a notification, notice, or posting required under this section would impede a criminal investigation or cause damage to national security, such notification, notice, or posting shall be delayed in the same manner as provided under section 164.528(a)(2) of title 45, Code of Federal Regulations, in the case of a disclosure covered under such section.

H. **Unsecured Protected Health Information**.—

(i) **Definition**.—

(A) **In General**.—Subject to subparagraph (B), for purposes of this section, the term ''unsecured protected health information'' means protected health information that is not secured through the use of a technology or methodology specified by the Secretary in the guidance issued under paragraph (2).

(B) **Exception in Case Timely Guidance Not Issued**.— In the case that the Secretary does not issue guidance under paragraph (2) by the date specified in such paragraph, for purposes of this section, the term ''unsecured protected health information'' shall mean protected health information that is not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

(2) **Guidance**.—For purposes of paragraph (1) and section 13407(f)(3), not later than the date that is 60 days after the date of the enactment of this Act, the Secretary shall, after consultation with stakeholders, issue (and annually update) guidance specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals, including the use of standards developed under section 3002(b)(2)(B)(vi) of the Public Health Service Act, as added by section 13101 of this Act.

I. **Report to Congress on Breaches**.—

(1) **In General**.—Not later than 12 months after the date of the enactment of this Act and annually thereafter, the Secretary shall prepare and submit to the Committee on Finance and the Committee on Health, Education, Labor, and Pensions of the Senate and the Committee on Ways and Means and the Committee on Energy and Commerce of the House of Representatives a report containing the information described in paragraph (2) regarding breaches for which notice was provided to the Secretary under subsection (e)(3).

(2) **Information.—t**he information described in this paragraph regarding breaches specified in paragraph (1) shall include—

(A) The number and nature of such breaches; and

(B) Actions taken in response to such breaches.

If you believe your PHI information has been breached in any way you may contact the Secretary of Health and Human Services or Allergy Consultants by notifying our Privacy Officer regarding your complaint. We will not retaliate against you for filing a complaint.

You may contact our Security Officer, Barbara Faupel, at **(314) 569-1881** for further information about the complaint process. This notice was published and becomes effective on or after May 18, 2023.