SAPPHIRE
Health & Wellness

Health Insurance Portability and Accountability Act (HIPAA)

OVERVIEW

HIPAA is the acronym for the *Health Insurance Portability and Accountability Act* of 1996. The purpose of this federal law was to improve portability of health insurance coverage, reduce healthcare fraud and abuse, and to protect the privacy of personal health records.

The federal agency responsible for putting HIPPA into action is the U.S. Department of Health and Human Services (DHHS). DHHS administers HIPAA by publishing federal regulations (also known as *rules*) and setting deadlines for organizations to comply. DHHS has put in effect several sets of regulations since HIPPA first went into effect.

In January 2013, DHHS enacted a significant update called the HIPPA Omnibus Rule (also referred to as the HIPAA *Mega Rule*). It marked the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented. This *Mega Rule* provided the public with increased control over personal health information and fortified privacy, security, breach notification and enforcement rules.

HIPPA and the HITECH Act

The HIPPA Omnibus Rule reflects significant modifications that were mandated by the HITECH Act (Health Information Technology for Economic and Clinical Health). HITECH is part of the American Recovery and Reinvestment Act of 2009 (ARRA). ARRA contained incentives related to health care information technology in general and contained specific incentives designed to accelerate the adoption of electronic health record systems among providers. As healthcare providers move toward exchanging large amounts of health information electronically, the HITECH Act put in place safeguards to ensure that individual information remains private and secure.

Definition of Terms

Covered Entities: HIPAA rules apply only to individuals, organizations and agencies that meet HIPAA's definition of a *covered entity*. Covered entities are defined in the HIPAA rules as the following:

- **Health Care Providers** –includes hearing health care.
- **Health Plans** –group health plans, certain long-term care plans, insurers, and HMOs.
- **Health Care Clearinghouses** –independent organizations that receive insurance claims from health care providers and redistributes the claims electronically to various insurance carriers.

Personal Health Information (PHI): PHI includes all individually identifiable health information in any form, electronic or non-electronic, that is held or transmitted by a covered entity, including oral communications. PHI includes demographic information collected from an individual that identifies, or can reasonably be used to identify, an individual. Examples of PHI are as follows (not an exhaustive list):

SAPPHIRE
Health & Wellness

- Name
- Address
- Dates (such as birthday, date of service, etc.)
- Phone/fax number
- E-mail address
- Social security number
- Medical record number
- Insurance information
- Account number
- License number
- Device serial number

The HIPAA Privacy Rule: Refers to a set of national standards that became finalized law in 2003 and received a major enhancement in 2013 through the HIPPA Omnibus Rule. The Privacy Rule protects the privacy of patients' medical records and other health information maintained by covered entities.

INDIVIDUAL RIGHTS UNDER HIPAA

The HIPAA Privacy Rule sets standards with respect to the rights of individuals to their health information, procedures for exercising those rights, and the authorized and required uses and disclosures of such information. Individuals have the right to:

Receive a Copy of a Covered Entity's Notice of Privacy Practices. The written notice must provide a clear, user-friendly explanation of the individual's rights with respect to his or her personal health information and the covered entity's privacy practices.

Request Restrictions on PHI. Individuals have the right to request restrictions regarding the use and disclosure of their PHI for treatment, payment, and healthcare operations. The law also grants individuals the right to request restrictions for other disclosures, such as those made to family members. Covered entities are NOT required to agree to the restrictions requested.

The HIPAA Omnibus Rule and HITECH Act take the request for restrictions one step further, and require that "a covered entity must agree to the request of an individual to restrict disclosure of PHI about the individual to a health plan if the disclosure is for the purposes of carrying out payment or health care operations and not otherwise required by law; and the PHI pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full."

Inspect and/or Receive A Copy of His or Her PHI. The Privacy Rule (with few exceptions) gives individuals the right to inspect, review, and receive a copy of his or her PHI (for example, medical and billing records). If an individual requests a copy of his or her PHI, the covered entity is allowed to charge a reasonable fee for the cost of supplies, labor, and postage. Individuals requesting copies from our company may be charged.

Actual postage costs may be added if the individual would like the information mailed to him or her. If the individual requests an alternative format, we will charge a cost-based fee for providing him or her health information in that format. If the individual prefers, we will prepare a summary or an explanation of his or her health information for a fee. Individuals may contact us for a full explanation of our fee structure.

The HITECH-HIPAA Omnibus Rule expands this right, giving individuals the right to access their own e-health record in an electronic format and to direct the covered entity to send the e-health record directly to a third party. The covered entity may only charge for labor and electronic transfer costs.

SAPPHIRE
Health & Wellness

Request Corrections to PHI. If an individual thinks the information in his or her medical or billing record is incorrect, he or she can request that our company amend the record. We are required to respond to requests and make changes to inaccurate or incomplete information. This rule also applies to a person authorized to act on behalf of the individual in making health care related decisions such as the individual's personal representative.

Obtain an Accounting of Disclosures. Under HIPAA, covered entities are required to track disclosures of PHI. The purpose of tracking disclosures is to give an individual the right to receive a written account of when and with whom his or her information has been shared within the six years prior to the date of their request. If files are maintained electronically, the tracking period is limited to disclosures made within a three-year period.
When requested, the covered entity must either:

- Provide an individual with an accounting of such disclosures made by the covered entity and all of its business associates.
- Provide an individual with an accounting of the disclosures made by the covered entity and a list of business associates, including their contact information, and who will be responsible for providing an accounting of such disclosures upon request.

Not all disclosures require tracking or need to be accounted for upon request by an individual. We are NOT required to track disclosures made for:

- Treatment, payment, and healthcare operation purposes.
- To the individual.
- To persons involved in the individual's care.
- National security or intelligence purposes or to correctional institutions or law enforcement officials.

File a Complaint. A patient has the right to complain if he or she feels that anyone in our company used or disclosed his or her PHI inappropriately. Patients can make us aware of concerns by contacting our Compliance Officer or by submitting a written complaint to the US Department of Health and Human Services. We support our patients' right to privacy of PHI and will NOT retaliate in any way if they choose to file a complaint.

Receive Notice of a Breach. Affected individuals have the right to be notified if there has been an unauthorized acquisition, access, use or disclosure of unsecured PHI in a manner not permitted by the Privacy Rule. He or she must receive notification without unreasonable delay, and in no case later than 60 calendar days after discovery of the breach.

OUR ORGANIZATION'S RESPONSE TO HIPAA

As HIPAA regulations evolve and update, we are required and committed to enhancing and changing our policies and practice as necessary. This guide describes our current policies and procedures.

Compliance Officer

There is a need to create a standardized and uniform approach to the handling of PHI. To meet this need, one individual fulfills the role of our company's Compliance Officer. The Compliance Officer is responsible for the development, implementation and maintenance of our privacy and compliance-related activities. The Compliance

Officer ensures that PHI is protected from unauthorized access yet remains accessible to individuals and to staff carrying out care and treatment. Contact information for our Compliance Officer is as follows:

Compliance Officer: Andrea Robbins
Phone: 480-219-7810
Email: andrea.robbins@sapphirehealthaz.com
Address: 3530 S Val Vista Dr Suite A111 Gilbert, AZ 85297

Workforce Training and Oversight
It is our company's policy to train all members of our workforce who have access to PHI on our privacy policies and procedures. Employees are required to review a HIPAA and HITECH training video to gain a full understanding of the general HIPAA privacy procedures, read and follow this training manual, and adhere to any other requirements and participate in mandatory trainings that may be dictated directly by HIPAA or the Compliance Officer.

Whenever a privacy incident has occurred, the Compliance Officer will evaluate the occurrence to determine whether additional staff training is in order. Any training developed to respond to the incident will be reviewed by the Compliance Officer to ensure it adequately addresses the incident and reinforces the company's privacy policies and procedures.

Patient Notification and Acknowledgement
All of our patients receive written notice of our privacy practices. In most cases the notice will be given to the patient on his or her first visit to us. The notice describes how we use and disclose patient PHI, the patient's right to access to his or her PHI, and our legal duties concerning PHI. Patient notification is accomplished as follows:

Paper Notification and Acknowledgment: We offer our patients a handout that gives notice of our privacy practices. HIPAA law requires we ask each patient to state in writing that they have received the notice. The law does NOT require patients to sign the acknowledgment of receipt of privacy practices. If a patient refuses to sign the acknowledgement we are required to keep a record that we made a good faith effort to obtain the patient's signature. Space to record the patient's acknowledgment of receipt of our Privacy Practices Notice is part of our intake form or can be recorded on a standalone form.

Electronic Notification and Acknowledgment: When a patient has received electronic notification of our privacy practices, an electronic return receipt or other return transmission from the individual is considered a valid written acknowledgment of the notice. A provider who gives paper notice to a patient during a face-to-face encounter may obtain an electronic acknowledgment from the individual, provided that the individual's acknowledgment is in writing. Thus, a receptionist's notation in the provider's computer system of the individual's receipt of the notice would NOT be considered a valid written acknowledgment.

Posted Notification: All offices or other physical sites where we provide care directly to individuals are required to post a notice of privacy practices in its entirety. The posted notice must be in a clear and prominent location. HIPAA rules do not prescribe any specific format for the posted notice, just that it includes the same information that is distributed directly to the individual. HIPAA rules allow us the discretion to design the posted notice in a manner that works best for each facility, which may be to simply post a copy of the notice that is distributed directly to individuals. However, in most situations our offices will use a 1-sided, enlarged, framed version of our handout to satisfy this rule.

Intimidation or Waiver Prohibited: No employee may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA. No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility.

Structural Safeguards

The HIPAA Privacy Rule is NOT intended to prohibit providers from talking to each other or to their patients; nor are we required to retrofit offices to provide private rooms or soundproof walls to avoid any possibility that a conversation is overheard. Provisions of this Rule do require us to take reasonable steps such as the following to ensure privacy and security:

- Staff should ask waiting customers to stand a few feet back from the desk used for patient counseling, check-ins or payments.
- Staff should make every effort to cover up patient records at the front desk while other patients are in the waiting area.
- The physician should use a private office to discuss the outcome of a test, to counsel, and otherwise treat patients when available and practicable.
- Areas that house paper with PHI on them should be supervised or locked.
- Office doors should be checked to ensure that they are locked and papers with PHI are put away before employees leave areas that house patient files unattended.
- Patient records containing PHI should be secured so that they are not readily available to those who do not need them.
- Papers containing PHI, which are slated to be discarded, should be shredded immediately or as soon as reasonable possible.

USE, DISCLOSURE AND PRECAUTION GUIDELINES

Many customary health care communications and practices play an important or even essential role in ensuring that individuals receive prompt and effective health care. Due to the nature of these communications and practices, as well as the various environments in which individuals receive health care or other services from covered entities, the potential exists for an individual's health information to be disclosed incidentally.

For example, a visitor may overhear a provider's confidential conversation with another provider or a patient or may glimpse a patient's information on a sign-in sheet. The HIPAA Privacy Rule is not intended to impede these customary and essential communications and practices. Rather, the Privacy Rule permits certain incidental uses and disclosures of PHI to occur when the covered entity has in place reasonable safeguards and minimum necessary policies and procedures to protect an individual's privacy.

HIPAA's privacy regulations permit covered entities to use and disclose PHI *WITHOUT* first obtaining written authorization from the patient as follows:

- As necessary to carry out medical treatment, payment or health care operations.
- To the patient.

SAPPHIRE
Health & Wellness

- To a patient's family member or personal representative. (Certain restrictions apply. See section on Family Members for details.)
- Pursuant to, and in compliance with, the patient's authorization.
- In certain other instances without the individual's consent, authorization or opportunity to object.

Treatment, Payment, and Health Care Operations

To avoid interfering with an individual's access to quality health care or the efficient payment for such health care, the Privacy Rule permits a covered entity to use and disclose PHI, with certain limits and protections, for treatment, payment and health care operations activities.(Certain exceptions apply in instances where the PHI in question is psychotherapy notes.) Examples of this type of permitted use are as follows:

Scheduling and Reports: Health care providers, such as a specialist or hospital to whom a patient is referred for the first time, are permitted to use an individual's PHI to set up appointments, schedule surgery, or other procedures without first obtaining the patient's written consent.

Consultations Between Providers: Consultation about a patient's condition is permitted between health care providers without the obtaining a patient's written authorization. In addition, a health care provider (or other covered entity) is expressly permitted to disclose PHI about an individual to a health care provider for that provider's treatment of the individual.

Confidential Conversations: The HIPAA Privacy Rule is not intended to prohibit providers from talking to each other and/or to their patients even if there is a possibility that the conversation could be overheard. The Privacy Rule recognizes that overheard communications in some settings may be unavoidable and allows for some incidental disclosures. The following examples of confidential communication are permissible under the Privacy Rule, if reasonable precautions are taken to minimize the chance of incidental disclosures to others who may be nearby:

- Orally coordinating services at the front desk.
- Discussing a patient's condition over the phone with the patient, a provider, or a family member.
- Discussing diagnostic hearing test results with a patient or other provider in a joint treatment area while another patient is present.
- Discussing a patient's condition with a dispenser trainee as part of their training.

In the examples above, reasonable precautions may include using lowered voices or talking apart from others. We are free to engage in communications as required for quick, effective, and high-quality health care.

Sign-in Sheets and Calling Out Names: HIPAA rules allow us to use patient sign-in sheets or call out patient names in waiting rooms so long as the information disclosed is appropriately limited. The HIPAA Privacy Rule explicitly permits the incidental disclosures that may result from this practice; for example, when other patients in a waiting room hear the identity of the person whose name is called, or see other patient names on a sign-in sheet. However, these incidental disclosures are permitted only when the covered entity has implemented reasonable safeguards and the minimum necessary standard, where appropriate. Reasonable safeguards include the following:

SAPPHIRE
Health & Wellness

- Sign in sheets may only include the minimum amount of PHI necessary to call the patient and must specifically exclude diagnostic information. For example, the sign- in sheet may NOT display medical information that is not necessary for the purpose of signing in (e.g., the specific problem for which the patient is being seen).
- Computer screens with patient information must be kept secure and turned away from the patients.
- When speaking to patients in the waiting room, staff will encourage patients to come to the front desk to receive further instructions in a more confidential manner.

Patient Records: The HIPAA Privacy Rule does not prohibit engaging in common and important health care practices; nor does it dictate the specific measures that must be applied to protect an individual's privacy while engaging in these practices.

Reasonable steps we take when accessing patient records are as follows:

- Staff accessing patient records outside of exam rooms will make sure the patient records are not visible to others.
- Staff will lock or log off computers or mobile devices when not attended
- Staff will ensure paper records are physically secured at all times.
- Staff will not share usernames and passwords
- Staff will note take photos of patients unless they are for medical or business reasons
- Staff will not discuss patient care on social media or engage in discussion with a patient about their care on social media

Medical Trainees: The definition of health care operations in the Privacy Rule provides for conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers. Covered entities can shape their policies and procedures for minimum necessary uses and disclosures to permit trainees access to patients' medical information, including entire medical records. Trainees (such as interns or residents) are allowed to access patient medical information as part of their training.

Fax and E-mail Communications

The HIPAA Privacy Rule permits us to communicate PHI to another health care provider for treatment purposes by way of fax, e-mail or other means. We must have in place reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of PHI that is disclosed.

Fax Safeguards

- Sender must verify that the fax number to be used is in fact the correct one for the health care provider.
- Use an electronic fax rather than manually faxing when possible.
- Outgoing facsimile transmissions may contain the following disclaimer on the fax cover page:

Confidentiality Notice: This message is intended only for the use of the individual or entity to which it is addressed and may contain Protected Healthcare Information. If you are not the intended recipient, be advised that any unauthorized use, disclosure, copying, distribution, or the taking of any action in reliance on the

contents of this information is strictly prohibited. If you have received this transmission in error, please immediately notify the sender via telephone or return fax.

E-mail Safeguards

- Review email recipient names before hitting "send"
- If the e-mail contains clinically relevant information, the sender must print a copy of it and place it in the patient's medical records.
- Review
- The following e-mail disclaimer may be added to every outgoing e-mail:

Confidentiality Notice: This e-mail is intended only for the use of the individual or entity to which it is addressed and may contain Protected Healthcare Information. If you are not the intended recipient, be advised that any unauthorized use, disclosure, copying, distribution, or the taking of any action in reliance on the contents of this information is strictly prohibited. If you have received this e-mail in error, please immediately notify the sender via telephone or return e-mail.

Minimum Necessary Policy

It is our company's policy to allow our physician and staff to have access to the level of PHI (minimum necessary or entire record) as is required to fulfill proper treatment, payment, and operation functions.

Minimum Necessary: When using, disclosing, or requesting PHI from another covered entity, the Privacy Rule requires a covered entity to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose. The determination of what constitutes minimum necessary data is left to the judgment of the covered entity.

Entire Records: The Privacy Rule does NOT prohibit the use, disclosure, or request of an entire medical record. A covered entity may use, disclose, or request an entire medical record without a case-by-case justification if the covered entity has documented in its policies and procedures that the entire medical record is the amount reasonably necessary for certain identified purposes.

Family Members, Personal Representatives and Power of Attorney

HIPAA rules do NOT require covered entities to obtain written permission before sharing or discussing PHI with a patient's family members, friends, or others involved in a patient care or payment for care. However, occasionally we may prefer or require that patients give written permission. If the patient is present and has the capacity to make health care decisions, a health care provider may discuss the patient's health information with others if the patient agrees or, when given the opportunity, does not object. A health care provider also may share information with these persons if, using professional judgment, he or she decides that the patient does not object. In either case, the health care provider may share or discuss only the information that the person involved needs to know about the patient's care or payment for care.

Obtaining PHI of a Deceased Family Member: The HIPAA Privacy Rule recognizes that a deceased individual's PHI may be relevant to a family member's health care. The Rule allows covered entities to release the PHI of a deceased relative to a surviving family member under the following circumstances:

SAPPHIRE
Health & Wellness

- **PHI is to be Used For Treatment Purposes:** Using PHI from one individual in the treatment of another individual does not require an authorization. Thus, a covered entity may disclose a decedent's PHI, without authorization, to the health care provider who is treating the surviving relative.

- **Authorized Disclosure:** 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.

Parents and Children: The Privacy Rule generally allows a parent to have access to the medical records about his or her child, as his or her minor child's personal representative when such access is not inconsistent with state or other law. However, there are situations when the parent would NOT be the minor's personal representative under the Privacy Rule. These situations are as follows:

- When the minor is the one who consents to care and the consent of the parent is not required under state or other applicable law.

- When the minor obtains care at the direction of a court or a person appointed by the court.

- When, and to the extent that, the parent agrees that the minor and the health care provider may have a confidential relationship.

Even in these exceptional situations, the parent may have access to the medical records of the minor when state or other applicable law requires or permits such parental access. Parental access would be denied when state or other law prohibits such access.

Finally, as is the case with respect to all personal representatives under the Privacy Rule, a provider may choose not to treat a parent as a personal representative when the provider reasonably believes, in his or her professional judgment, that the child has been or may be subjected to domestic violence, abuse or neglect, or that treating the parent as the child's personal representative could endanger the child.

Power of Attorney: The Privacy Rule provisions regarding personal representatives generally grant persons, who have authority to make health care decisions for an individual under other law, the ability to exercise the rights of that individual with respect to health information.

Non-applicable Power of Attorney: Power of attorney given to a person for purposes other than health care, such as a power of attorney to close on real estate, does NOT authorize the holder to exercise the individual's rights under the HIPAA Privacy Rule.

Further, a covered entity does not have to treat a personal representative as the individual if, in the exercise of professional judgment, it believes doing so would not be in the best interest of the individual because of a reasonable belief that the individual has been or may be subject to domestic violence, abuse or neglect by the personal representative, or that doing so would otherwise endanger the individual.

Except with respect to decedents, a covered entity must treat a personal representative as the individual only when that person has authority under other law to act on the individual's behalf on matters related to health care.

SAPPHIRE
Health & Wellness

Business Associates

The HIPAA Privacy Rule applies only to covered entities (health plans, health care clearinghouses, and health care providers). However, most covered entities do not carry out all of their health care activities and functions by themselves. Instead, they often use the services of a variety of other persons or businesses, which HIPAA refers to as *business associates*.

The Privacy Rule allows covered entities to disclose PHI to business associates if the covered entity obtains satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule.

Covered entities may disclose PHI to an entity in its role as a business associate only to help the covered entity carry out its health care functions—not for the Business Associate's independent use or purposes, except as needed for the proper management and administration of the Business Associate.

Examples of our business associates receiving PHI include those individuals providing non-treatment services such as janitorial staff, document destruction, coding and billing contractors. When disclosing PHI to business associates it is our policy to

- Make reasonable efforts to limit PHI disclosures to the minimum necessary to provide treatment, receive payment, or conduct health care operations.
- If there is any indication that a business associate receiving PHI is, or may be using, the information in a manner that is inconsistent with the services requested, immediately notify the Compliance Officer to investigate the concern.
- Employees are prohibited from selling or providing PHI to business associates for marketing purposes as defined by HIPAA (see Marketing Communications Under HIPAA section for details).

Business Associate Agreements

The HIPAA Privacy Rule does NOT hold covered entities liable for, or require them to monitor, the actions of its business associates. It requires we enter into written contracts or other arrangements with business associates that protect the privacy of PHI. We are NOT required to monitor or oversee the extent to which the business associate abides by the privacy requirements of the contract.

However, if a covered entity finds out about a material breach or violation of the contract by the Business Associate, it must take reasonable steps to cure the breach or end the violation. If unsuccessful, the contract with the business associate must be terminated. If termination is not feasible (e.g., where there are no other viable business alternatives for the covered entity), the covered entity must report the problem to the Department of Health and Human Services Office for Civil Rights.

With respect to business associates, the HIPAA Privacy Rule considers a covered entity out of compliance if it fails to take the steps described above. If a covered entity's out of compliance with the Privacy Rule because of its failure to take these steps, further disclosures of PHI to the business associate are not permitted.

SAPPHIRE
Health & Wellness

Instances When Business Associate Agreements are NOT Needed

Treatment Purposes: Health care providers often have business associate relationships with other health care providers. The HIPAA Privacy Rule explicitly excludes them from needing a business associate agreement because their disclosures are made for treatment purposes. Therefore, any covered health care provider (or other covered entity) may share PHI with a health care provider for treatment purposes *WITHOUT* a business associate contract.

However, this exception does not preclude one health care provider from establishing a business associate relationship with another health care provider for some other purpose. For example, a hospital may enlist the services of another health care provider to assist in the hospital's training of medical students. In this case, a business associate contract *WOULD BE REQUIRED* before the hospital could allow the health care provider access to patient health information.

Inadvertent Contact: A business associate contract is *NOT* required with persons or organizations whose functions, activities, or services do not involve the use or disclosure of PHI, and where any access to PHI by such persons would be incidental, if at all

Health Providers and Health Plan or Payer: Generally, providers are not business associates of payers. For example, if a provider is a member of a health plan network and the only relationship between the health plan (payer) and the provider is one where the provider submits claims for payment to the plan, then the provider is not a business associate of the health plan. Each covered entity's acting on its own behalf when a provider submits a claim to a health plan, and when the health plan assesses and pays the claim. However, a business associate relationship could arise if the provider is performing another function on behalf of, or providing services to, the health plan (e.g., case management services) that meet the definition of "Business Associate."

Public Health Provision

The HIPAA Privacy Rule recognizes the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to an individual's PHI to carry out their public health mission. The Rule also recognizes that public health reports made by covered entities are an important means of identifying threats to the health and safety of the public at large, as well as individuals. Accordingly, the Rule permits covered entities to disclose PHI without authorization for specified public health purposes.

Please Note: The Privacy Rule's public health provision ***permits*** but ***does not require*** covered entities to make the public health disclosures described above. This provision is intended to allow covered entities to continue current voluntary reporting practices that are critically important to public health and safety. The Rule also permits covered entities to disclose PHI when state or other law requires covered entities to make disclosures for public health purposes.

Disclosure of Findings to Employers. The public health provision permits covered health care providers to disclose an individual's PHI to the individual's employer *WITHOUT* authorization in very limited circumstances. These circumstances include:

- The covered health care provider has provided the health care service to the individual at the request of the individual's employer or as a member of the employer's workforce.
- The health care service provided relates to the medical surveillance of the workplace or an evaluation to determine whether the individual has a work- related illness or injury.

- The employer has a duty under the Occupational Safety and Health Administration (OSHA), the Mine Safety and Health Administration (MSHA), or the requirements of a similar State law, to keep records on or act on such information.

Generally, pre-placement physicals, drug tests, and fitness-for-duty examinations are not performed for such purposes described above. However, to the extent such an examination is conducted at the request of the employer for the purpose of such workplace medical surveillance or work-related illness or injury, and the employer needs the information to comply with the requirements of OSHA, MSHA, or similar State law, the PHI the employer needs to meet such legal obligation may be disclosed to the employer without authorization. Covered health care providers who make such disclosures must provide the individual with written notice that the information is to be disclosed to his or her employer (or by posting the notice at the worksite if the service is provided there).

Workers' Compensation and Judicial/Administrative Proceedings Workers' Compensation: The HIPAA Privacy Rule does NOT apply to entities that are workers' compensation insurers, workers' compensation administrative agencies, or employers, except to the extent they may otherwise be covered entities. However, these entities need access to the health information of individuals who are injured on the job or who have a work-related illness to process or adjudicate claims, or to coordinate care under workers' compensation systems. Generally, this health information is obtained from health care providers who treat these individuals and whom the Privacy Rule may cover.

The Privacy Rule recognizes the legitimate needs of the workers' compensation systems to have access to PHI as authorized by state or other law. Due to the significant variability among state laws, the Privacy Rule permits disclosures of health information for workers' compensation purposes without the individual's authorization to the extent disclosure is required by state or other law. The disclosure must comply with and be limited to what the law requires. Disclosure is permitted if an individual has provided his or her authorization for the release of the information to the entity. Individuals do NOT have a right under the Privacy Rule to request that a covered entity restrict a disclosure of his or her PHI if it is required by law and necessary to comply with workers' compensation or a similar law.

Judicial/Administrative Proceedings: The Privacy Rule generally permits covered entities to disclose an individual's PHI without first obtaining the individual's consent or offering him or her the opportunity to agree or object in the course of any judicial or administrative proceeding in response to a court order, subpoena, or other lawful process.

MARKETING COMMUNICATIONS UNDER HIPAA

Marketing generally means a communication about a product or service that encourages the individual to purchase or use the product or service. The HIPAA Privacy Rule gives individuals important controls over whether and how their PHI is used and disclosed for marketing purposes.

Written Authorization

With limited exceptions, the HIPAA Privacy Rule requires an individual's written authorization before use or disclosure of his or her PHI (which includes full face photos) can be made for marketing. Examples of marketing activities prohibited without written authorization from the individual would be to

SAPPHIRE
Health & Wellness

- Provide list of names of patients who have undergone cosmetic treatments to plastic surgeons for the surgeon's promotions without the patient's authorization
- Use photos of patients who have undergone chemical peels on a brochure without first obtaining the patient's authorization.

Financial Remuneration Rules

Under HIPAA's Privacy Rule, merely having a "financial relationship" between the third party and the covered entity is not sufficient by itself to implicate the rule. Instead, under HIPAA's Privacy Rule the purpose of the financial remuneration must specifically be to pay the covered entity to make a communication that encourages individuals to purchase or use the third party's product or service. For example, a covered entity would not need to obtain authorizations prior to sending communications encouraging individuals to participate in another clinic's disease management program, even if the clinic provided financial remuneration to the covered entity to implement the program, as long as the communications were directing individuals to the clinic's program, and not the clinic's product or service.

ENFORCEMENT AND VIOLATIONS

Questions and Complaints

The Compliance Officer is responsible for creating a process for individuals to inquire about our company's privacy practices, lodge complaints and for handling such complaints.

Violations

In the event of a security incident that results in a wrongful disclosure of PHI, the Compliance Officer, will take appropriate actions to prevent further inappropriate disclosures. In addition, Legal Counsel may be consulted as part of the review team to assist in the review and investigation of privacy incidents when required.

If the Compliance Officer has not resolved the incident, the Compliance Officer shall involve anyone determined to be necessary to assist in the resolution of the incident. If participants need to be notified of any lost/ stolen PHI, the Compliance Officer will send PHI theft/loss disclosure letters to all possible affected individuals.

Breach Notifications

Under the HITECH Act covered entities and business associates are required to notify affected individuals if there is an unauthorized acquisition, access, use, or disclosure of unsecured PHI, subject to certain limited exceptions. PHI is considered unsecured unless it is encrypted or destroyed through the use of methodologies and technologies specifically approved in guidance issued by the US Department of Health and Human Services (DHHS).

If unsecured PHI has been breached, affected individuals must be notified by first-class mail or by e-mail if the individual specifies e-mail. If contact information for fewer than 10 individuals is insufficient or out-of-date, notice of the breach may be accomplished by an alternative form of written notice such as by telephone or other means. If a posted notice on the homepage of our website (or through a hyperlink on its homepage) is used as a breach notice it will remain for 90 days or publish a conspicuous notice in print or broadcast media in geographic areas where individuals affected by the breach reside.

If more than 500 individuals in a single state or jurisdiction are affected, notice must be provided to prominent media outlets serving such state or jurisdiction (e.g., in the form of a press release). If there exists the possibility of imminent misuse of the unsecured PHI, telephone calls to affected individuals may also be appropriate.

Notifications must be made without unreasonable delay and in no case later than 60 calendar days after discovery of the breach. The notice must include certain specific information.

If the breach involves 500 or more individuals, DHHS must be notified immediately, which will subsequently post the breach on its website. If the breach involves less than 500 individuals, the covered entity must maintain a log and submit the log to DHHS on an annual basis.

Sanctions for Failing to Comply

Failure to comply with HIPAA can result in civil and criminal penalties.

Civil Penalties: There is a tiered civil penalty structure for HIPAA violations. The Secretary of the Department of Health and Human Services (DHHS) has discretion in determining the amount of the penalty based on the nature and extent of the violation and the nature and extent of the harm resulting from the violation. The Secretary is prohibited from imposing civil penalties (except in cases of willful neglect) if the violation is corrected within 30 days (this time period may be extended).

Criminal Penalties: Covered entities and specified individuals whom "knowingly" obtain or disclose PHI face a fine of up to $50,000, as well as imprisonment up to one year. Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, with up to five years in prison. Finally, offenses committed with the intent to sell, transfer, or use PHI for commercial advantage, personal gain or malicious harm permit fines of $250,000, and imprisonment for up to ten years.

Workforce Disciplinary Actions: Our Company will take the following actions when an employee fails to comply with our HIPAA policies and procedures.

- **First Offense:** Verbal and written warning with explanation of specific violation or violations.
- **Second Offense:** Second verbal and written warning and retraining of policies and procedures at employees' expense.
- **Third Offense:** Termination of employment.