TeleMedik	Confidentiality in the Management of Privileged Information	
Policy Code: **ADM COMP 002**	Effective Date: 02/2002	Latest Review: 10/2018
Responsible Officer: Position	Edgar Ramírez Compliance & Privacy Officer	
Authorization: Position	Nilda Guerrero Executive Director	
Next Review: 10/2019		*This policy will be reviewed annually.*

Scope

This policy is company-wide; it applies to all regular and temporary employees within the organization, including committee members, Board of Directors, consultants, operational and administrative areas. It also extends to our clients and providers, vendors, contractors, and sub-contractors that provide professional services to our organization.

Policy

This policy establishes the procedure to handle the Management of Confidential Information, annual revision process for compliance with this policy, how to use the fax when sending PHI information and its retention period.

Purpose

Our purpose is to ensure the confidentiality, privacy, integrity, availability and security of all privileged information (including but not limited to PHI information) that TeleMedik and/or any of its affiliates creates, receives, maintains or transmits. Through this and other policies, we ensure the protection of such information with legal and technological resources of security breaches, threats, use or unauthorized disclosure that are of our knowledge. We understand that the demonstrated ability to handle the confidential information of our customers is one of the main assets of our business.

All members of the services we offer to TeleMedik clients and/or any of their affiliates, who receive services provided by any of our employees; have the right to have all of the individual's identifiable information, provided verbally or in writing, through of the telephone, fax or computer system is handled with strict confidentiality and privacy.

Policy Background and Legal Basis

This policy ensures that TeleMedik and/or any of its affiliates complies with laws such as HIPAA and current regulations, especially those of the health industry established by OIG and CMS.

We also ensure the protection of information according to *Ley 246 para la Seguridad, Bienestar y Protección de Menores en su Artículo 26, la ley 121 Ley de la Carta de Derechos de la Persona de Edad Avanzada y la Ley 238 Carta de Derechos de las Personas con Impedimentos.*

Other stipulations are established by our accrediting entities and by URAC, NCQA & ATA and by our clients, who are also governed by state and federal regulations.

Definitions

HIPAA - Health Insurance Portability and Accountability Act (HIPAA) of 1996 establishes standards that rule Health Care Industry and provides sanctions or penalties for Organizations that do not comply with those standards. One of the primary purposes is to protect the personal health information of all individuals.

CMS – Centers for Medicare and Medicaid Services (CMS) is a US federal agency which administers Medicare, Medicaid, and the Children's Health Insurance Program.

NCQA - The National Committee for Quality Assurance (NCQA) is an independent non-profit organization in the United States designed to improve health care quality.

URAC- Utilization Review Accreditation Commission (URAC), an independent, nonprofit organization, is well-known as a leader in promoting health care quality through its accreditation, education and measurement programs.

PHI – Protected Health Information (PHI) as established by HIPAA.

FTP - File Transfer Protocol is a standard network protocol used to transfer computer files between a client and server on a computer network. FTP is built on a client-server model architecture and uses separate control and data connections

ATA - American Telemedicine Association – non-profit organization that promotes access to medical care for consumers and health professionals through telecommunications.

HITECH - Health Information Technology for Economic and Clinical Health - is a legislation that was created to stimulate the adoption of electronic health records (EHR) and the supporting technology including electronic health records and private and secure electronic health information exchange.

Participant – A person who is eligible to receive health benefits under a healthcare insurance or benefits or take part of a health service. The term participant in this regard may refer to a patient, an employee, or other dependents

Responsibilities

1. Supervisor/manager - Responsible for compliance of this policy. She/he must provide a fair application of this policy for all employees under her/his responsibility.
2. Human Resources and Compliance Officer - Responsible for the orientation and distribution of this policy. She/he assures the compliance of this policy providing

ORIGINAL

coaching to supervisors and managers. She/he receives and investigates all related concerns of employees to this policy and its compliance.

3. Information System Security Officer - responsible for the ongoing management of information security policies, procedures, and technical systems to maintain the confidentiality, integrity, and availability of all organizational healthcare information systems.
4. Employee - is responsible for the compliance with the practices established in this policy and be aware of possible compliance risks, especially those related to the prevention and detection of activities that fail to comply with the provisions of this policy.

Aspects to consider regarding this policy

Any specific requirement established by any of our clients will be included as an attachment to this policy. We understand that this policy covers all the requirements to enforce correctly and diligent management of any PHI. However, depending on the specific needs or policies of the clients, additional reinforcement measures will be provided to our employees.

Related Policies

ADM COMP 007 - Duties and Responsibilities of the Officers and the Compliance Committee
ADM CORP 023 - Management and Disposition of Confidential Documents
ADM CORP 037 - Business Associate Agreement
SYST PRI 001 - Data Integration and Interchange Policy
SYST SEC 002 - Data Encryption and Decryption
SYST SEC 003 - Disposal of Electronic Devices and Media Re-Use
SYST SEC 019 - HIPAA Data & Information Security Awareness and Training

Amendments

This policy may be modified if necessary, in compliance with applicable laws and regulations. The document is subject to contract changes for each client and any regulation required.

Separability Clause

If any word, section or part of this Protocol were to be declared unconstitutional or void by a court of law, such declaration will not affect the remaining dispositions or parts of this Protocol, rather its effect will be limited to the specific word, section or part of the Protocol declared void or

ORIGINAL

unconstitutional. The nullity or invalidity of any word, section or part of this Protocol will not be deemed as affecting in any way its application or validity in any other section or part of the document.

Attachments

☒ Yes ☐ No

Attachments included (if applicable)

Attachment A – Privacy Notice
Attachment B - *Acuerdo de Confidencialidad y No Conflicto de Interés*
Attachment C - *Certificación de recibo de Políticas Organizacionales*
Attachment D - Transmission methods procedure for sending PHI information
Attachment E - Fax Cover

ORIGINAL

PRIVACY NOTICE

Procedure for confidentiality in the management of privileged Information:

1. Protected Health Information (PHI) obtained by TeleMedik and/or any of its affiliates through media and received by company employees will only be disclosed in compliance with state and federal laws and applicable regulations for the disclosure of confidential information. Health related information will be obtained only by staff working for TeleMedik and/or any of its affiliates. The staff is composed of nurses, nutritionists, pharmacists, doctors, consultants, service representatives and administrative personnel who will manage protected health information through telephone, fax or computer system. The information obtained is the minimum necessary, limited only to that necessary to carry out the functions established by our customers in the contract. All personnel will require training and be oriented to comply with the correct management of protected health information. The required training related to Privacy and Security will be provided within the first 90 days of hiring the resource and then an annual review will be carried out.
2. TeleMedik and/or any of its affiliate's employees will use the information received for the only purpose of carrying out clinical activities or providing services offered by the company, by the health organization or insurance company for which it establishes contracts. The services or programs offered include, but are not limited to, the following: condition management, quality management, utilization management, discharge planning, network management, case management, telemedicine and prescription drug audits of the medical plans. In the case of shared activities between TeleMedik and other organizations or medical plans, TeleMedik will designate an organization authorized employee or company to receive and deliver the PHI. In case of doubts, will always consult and obtain the client's permission to use the information according to the client's specifications.
3. The Board of Directors, employees and contractors will annually sign a Confidential Agreement to guarantee the compliance with this policy. **Refer to Attachment B - *Acuerdo de Confidencialidad y No Conflicto de Interés.***
4. All temporary and regular employees employed by TeleMedik (including operational or employees with administrative functions and committee members) will receive orientation regarding Management of Confidentiality in Clinical Information, HIPAA and Hi-tech regulations (including provisions for Management of Protected Health Information or PHI); CMS regulations; Fraud, Lost and Abuse, among other applicable terms and policies. They will sign an agreement and/or attendance list as evidence of this discussion and will participate in compliance with the procedures described as part of their contract with TeleMedik. **Refer to Attachment C - *Certificación de recibo de Políticas Organizacionales***.
5. During the Welcome process of new employees, they will be informed that failure to comply with this policy, intentional or unintentional, will involve disciplinary actions that may include, in extreme cases, the termination of their employment relationship. Specific statements that support these requirements are defined as part of our Organizational Values and are part of our Code of Ethics and Conduct for Employees. This information is constantly reinforced to all employees as part of our Cultural Philosophy.

ORIGINAL

6. All existing employees will receive updates to this policy (changes may occur due to amendments to laws and regulations) and other related aspects at least annually during their contract period. They must sign a receipt as evidence of these reviews and take a test to measure the understanding of the topic discussed. A form of self-disclosure will be included as part of the annual reinforcement or review.
7. Any company, contractor and subcontractor (if any) will receive orientation and will also sign a confidentiality agreement as part of their contract with TeleMedik and/or any of its affiliates. **Refer to policy ADM CORP 037 - Business Associate Agreement.**
8. If the company, contractor and sub-contractor (if any) do not comply with this policy and/or related policies, the contract could be immediately cancelled, depending to the impact or non-compliance severity.
9. This policy, also our organizational and operational policies, will always be available in the Intranet for employees to review in any needed moment; the Human Resources Department, Compliance and Privacy Officer and/or its immediate supervisor will answer any questions to this matter.
10. If an employee has questions or concerns regarding to offering clinic information to any governmental agency, public or private social service, health organization or health insurance company, must consult with the supervisor prior to providing such information.
11. If an employee doesn't comply with this policy and/or related policies with respect to confidentiality of an PHI or any protected information, it will be subject to corrective actions such a, training, verbal corrective action, written corrective action or termination of employment. This action could vary according the severity of the non-compliance situation. The impact in the organization and/or to our clients will be considered during the evaluation.
12. The professional could share the PHI only in cases that the health or security of the person is at risk. This situation will be informed and explained to the personnel and area possible cases will be discussed specifically when managing crisis calls or mental related situations.
13. Any Exchange of information should be done using the secure methods available, for example the utilization of File Transfer Protocols (FTP).
14. In the case of having to send information using the e-mail, it will be sent encrypted.
15. In the case of sending documents via fax containing health confidential information, the employee will refer to the procedure on how to send PHI information and will use the TeleMedik official fax cover form. **Refer to Attachment D - Transmission methods procedure for sending PHI information and Attachment E - Fax Cover.**
16. Management of correspondence will be handled from the mailing room, which is always locked.
17. For the management and disposition of documents **Refer to policy ADM CORP 023 – Management and Disposition of Confidential Documents.**

Health information of participants may be used, disclosed and accessed according to the following:

1. Written requests and additional information - The participant may request additional information about TeleMedik privacy practices or obtain forms for submitting written requests by contacting the TeleMedik Compliance and Privacy Office: PMB 347 Ave. Winston Churchill #138, San Juan, P.R. 00926-6013 or toll-free by telephone at 1-787-999-6200. You can also send an e-mail to: compliance@telemedik.com to request additional information.
2. Obtain a Copy of the Notice - The participant has the right to obtain a copy of our current Notice at any time. The participant could access it directly in the application *TeleMedik Innova Health*

ORIGINAL

Solution, visiting our website: www.telemedik.com or contacting the TeleMedik Compliance and Privacy Office via e-mail at compliance@telemedik.com.

3. Inspect and obtain a copy of the PHI - With a few exceptions, the participant has the right to see and get a copy of the PHI we maintain about his/her. The participant may request access the PHI electronically. To inspect or obtain a copy of the PHI, the participant must submit a written request to the TeleMedik Compliance and Privacy Office. The participant may also ask us to provide a copy of the PHI to another person or entity. A reasonable fee may be charged for the expense of fulfilling your request as permitted under HIPAA and/or state law.
4. Request an amendment – The participant could request that we amend the protected information included in our systems. To request an amendment, submit a written request to the TeleMedik Compliance and Privacy Office. The participant must include a reason that supports your request.
5. Receive an accounting of disclosures – The participant has the right to request an accounting of disclosures we make of the PHI for purposes other than treatment, payment or health care operations. To obtain an accounting, the participant needs to submit a written request to the TeleMedik Compliance and Privacy Office. The participant may be charged for the cost of any subsequent accountings. In these cases, we will notify the participant in advance of the cost involved, and you may choose to withdraw or modify your request at that time.
6. Request confidential communications – The participant has the right to request that we communicate with him/her in a certain way or at a certain location. To request confidential communication of their PHI, participants must submit a written request to the TeleMedik Compliance and Privacy Office.
7. Request a restriction on certain uses and disclosures – Participant has the right to request additional restrictions on our use and disclosure of their PHI by sending a written request to the TeleMedik Compliance and Privacy Office.
8. Notification of Breach – The participant will be notified in the event there is a breach of the unsecured PHI as defined by HIPAA.

As Delegated Entity the Operational Area will proceed as the following:

1. In our operational areas, if the participant requests a written copy of a call made to our Center, should make the petition in writing to the attention of the Medical Insurance in which he is subscribed. In the case that the Health Agency (health plan) request such information, it will be provided in writing with the detail of the service offered and the result of the interaction.
2. In our operational areas, such as the Contact Center, if the participant requests a restriction on the use and disclosure of his/her file, demographic changes and/or disclosure reports must be referred to the insurance entity to which he/she is subscribed to manage the such request.
3. In the case that there are specific procedures related this rule by any of the clients to whom we offer services, those processes will be observed. There will be available as part of the training offered to functional areas, through access to specific information databases of the client or as part of our policies and/or procedures.

Additional Information:

- For any additional information regarding this procedure you should contact your supervisor, the Compliance and Privacy Officer and/or Executive Director.

ORIGINAL

- The participant can file a complaint with the TeleMedik Compliance and Privacy Office or with the Secretary of the United States Department of Health and Human Services, if believes their privacy rights have been violated. All complaints must be submitted in writing. The participant or complainant will not be penalized or otherwise retaliated against in any way for filing a complaint, according to our Policy ADM COMP 009 - Whistleblower Protection.

ORIGINAL