Union Health HIPAA Privacy and Security Plan

Board Approved - 11/20/2025

Table of Contents

INTRODUCTION

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) places restrictions on the access, use, and disclosure of individually identifiable health information which is information held or transmitted by Union Health or its business associate, in any form or media, whether electronic, paper, or oral and relates to the individual's past, present, or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual (collectively "PHI"). The HIPAA Privacy Rule safeguards all PHI, in any medium, and the HIPAA Security Rule safeguards electronic protected health information ("ePHI"). HIPAA protections extend to the PHI of deceased individuals.

It is Union Health's responsibility to comply fully with all HIPAA regulations and to ensure the privacy and security of all forms of PHI. All members of the workforce who have access to PHI are required to comply with this HIPAA Privacy and Security Plan ("Plan"). For purposes of this plan, the term "workforce" includes employees, volunteers, interns or trainees, board members, and other persons whose conduct, in the performance of work for Union Health or its business associate, is under the direct control of Union Health or its business associate, whether or not they are paid by Union Health or its business associate.

The Plan is essential for the management, accountability, and oversight structure of Union Health to ensure that proper safeguards and policies and procedures are in place for PHI.

I. HIPAA REGULATIONS

A. Privacy Rule

The Standards for Privacy of Individually Identifiable Health Information is known as the Privacy Rule. This federal rule was created to protect health information. It was also created to directly impact the Health Insurance Portability and Accountability Act of 1996 by addressing the use and disclosure of an individual's PHI held by organizations that are subject to the Privacy Rule called covered entities. The Privacy Rule also establishes individual's privacy rights which explain how covered entities use and disclose their information as well as provide individuals with more control over how that information is to be used.

A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high-quality health care and to protect the public's health and well-being.

B. Security Rule

The Security Standards for the Protection of electronic PHI is known as the Security Rule. This federal rule was created to protect health information that is held or transferred in electronic form. The Security Rule completes the protections contained within the Privacy Rule by addressing the technical and non-technical safeguards required to secure electronic PHI. Innovative technologies are evolving, and covered entities are relying on the use of electronic PHI for many core operations.

A major goal of the Security Rule is to protect the privacy of individuals' health information while allowing covered entities to adopt modern technologies to improve the quality and efficiency of patient care.

C. Enforcement Rule

The HIPAA Enforcement Rule refers to compliance with HIPAA and investigations, the obligation of monetary penalties for violations, and hearing procedures. The Enforcement Rule applies to all the HIPAA Rules.

D. Health Information Technology for Economical and Clinical Health Act (HITECH)

HITECH incentivized the adoption and use of health information technology. This regulation allowed patients to be more active in their healthcare, simplified the exchange of information, and strengthened privacy and security practices within HIPAA.

E. Breach Notification Rule

The Breach Notification Rule requires Union Health and its business associates to provide notification following a breach of unsecured PHI.

II. ADDITIONAL PRIVACY AND DATA PROTECTION LAWS AND GUIDANCE

A. The Office of the National Coordinator for Health Information Technology (ONC) Information Blocking Rule

The Information Blocking final rule eliminates intentional barriers to the electronic health information (EHI) exchange. This rule was designed to give patients greater control over their personal health data and make it easier to share patient records between organizations and with patients. Information blocking is a practice by an "actor" that is likely to interfere with the access, exchange, or use of EHI, except as required by law or specified in an information blocking exception. The Cures Act applied the law to healthcare providers, health IT developers of certified health IT, and health information exchanges (HIEs)/health information networks (HINs). There are exceptions to information blocking; when an actor's practice meets an exception, it will not be considered information blocking.

B. 42 C.F.R. Part 2 Confidentiality of Substance Use Disorder Patient Records

The 42 CFR Part 2 ("Part 2") regulations apply to covered entities that provide diagnosis, treatment, or referral for treatment of substance use disorders and are federally assisted programs. These regulations are designed to protect the privacy and confidentiality of individuals receiving substance use disorder treatment by imposing restrictions on the use and disclosure of patient-identifying information. Even when a healthcare organization is a HIPAA covered entity, Part 2 requirements remain applicable and, in many cases, are more stringent. Therefore, covered entities that maintain or receive information from a Part 2 program must ensure that disclosures comply with both HIPAA and Part 2, including obtaining proper patient consent or meeting a specific exception under the law. The intent of these regulations is to encourage individuals to seek treatment without fear that their sensitive information will be used against them in legal, employment, or social contexts.

C. The Cybersecurity and Infrastructure Security Agency (CISA)

CISA is a federal agency within the U.S. Department of Homeland Security responsible for enhancing the security, resilience, and reliability of the nation's critical infrastructure, including the healthcare sector. For a HIPAA-covered entity, CISA serves as a key resource and partner in protecting against cyber threats, such as ransomware, phishing, and data breaches that could compromise PHI. CISA provides guidance, threat intelligence, vulnerability alerts, and best practices to help strengthen cybersecurity posture. By leveraging CISA's tools and recommendations, such as the Health Sector Cybersecurity Coordination Center (HC3) alerts and the Cyber Hygiene Services program, Union Health can better align with HIPAA's Security Rule requirements to ensure the confidentiality, integrity, and availability of electronic PHI.

III. ADMINISTRATIVE REQUIREMENTS

A. Designation of Officers

Union Health has designated a Privacy Officer and a Security Officer who are responsible for aligning HIPAA policies and procedures, foster an organizational culture based on trust and safeguarding all forms of PHI, ensure that all members of the workforce are appropriately trained, and when necessary, coordinate breach and security incident response.

Privacy Officer. The HIPAA Compliance and Privacy Officer ("Privacy Officer') has the overall responsibility and accountability for ensuring the implementation of HIPAA regulations and any other applicable federal or state law relating to privacy and the oversight, maintenance, and enforcement of adherence to this Plan. This may include, but is not limited to, the development and implementation of policies and procedures, identification of business associates, and administers HIPAA training for all workforce members. The Privacy Officer shall also be responsible for implementing safeguards and maintaining the privacy and confidentiality of all information deemed necessary such as employment information and Plan. The Privacy Officer has a direct reporting line to the Chief Legal Officer with access to report to the President of Union Health and the Union Health Boards by way of the Board's Compliance Committee.

Contact information for the Privacy Officer:

Candie Cuffle
HIPAA Compliance and Privacy Officer
(812) 478-4188
caallen@union.health

Security Officer. The Security Officer is responsible for the ongoing management of information security policies, procedures, and technical systems. The Security Officer has a direct reporting line to the Chief Information Officer.

Contact information for the Security Officer:

George Mania
(Interim) Security Officer
(812) 238-7992
gmaina@union.health

B. HIPAA Training

Union Health provides HIPAA training to each workforce member on its policies and procedures, as necessary and appropriate for the workforce to carry out their functions at Union Health. Each new member of the workforce will be trained within 30 days of the start of their employment, and annually thereafter. In the event of a privacy incident, the Privacy Officer will collaborate with the appropriate department leader to determine if additional HIPAA training is necessary. In the event additional HIPAA training is necessary, it is at the discretion of the Privacy Officer what material shall be covered in the training. All workforce training will be documented.

C. Safeguards

Union Health has implemented the appropriate administrative, technical, and physical safeguards to protect the privacy of PHI. These safeguards provide reasonable protection from any intentional or unintentional use or disclosure that violates HIPAA and limit incidental uses and disclosures made under an otherwise permitted or required use or disclosure.

Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect health information and to manage the conduct of Union Health's workforce concerning the protection of that information. Physical safeguards are the physical measures, policies, and procedures implemented to protect information contained in our systems, buildings, and equipment from natural and environmental hazards and unauthorized intrusion. Technical safeguards are the technology and the policies and procedures for its use that protect health information and control access to it.

Union Health stays compliant with all HIPAA safeguards requirements by maintaining and executing policies and procedures including but not limited to annual risk assessments, data encryption, employee training, and business associate management.

D. Complaints

Union Health provides a process for individuals to make complaints concerning Union Health's HIPAA policies and procedures. All complaints are documented, and the disposition recorded. HIPAA complaints shall be directed to and managed by the Privacy Officer. The following methods may be used to submit a HIPAA complaint to the Privacy Officer:

- Contact the Privacy Officer directly.
- Department Privacy Email: privacy@union.health
- Department Phone: (812) 238-7533

- Compliance Line: 1-800-549-4623 or www.lighthouse-services.com/uhhg

An individual has a right to file a complaint to the Secretary if there is a belief that Union Health or its business associate is not complying with any of the HIPAA regulations. The Secretary will investigate a complaint when a preliminary review shows cause for a violation due to willful neglect and may investigate other complaints filed.

E. Sanctions

Union Health provides the appropriate sanctions for failing to comply with HIPAA privacy and security policies and procedures. Union Health has created a HIPAA Privacy and Security Sanction Policy to guide the appropriate sanction and assist in the consistency of the applied sanctions. All sanctions will be documented by the Privacy Officer.

F. Mitigation

Union Health mitigates, to the extent practicable, any harmful effect that is known to any workforce members of Union Health or its business associate, of the use or disclosure of PHI in violation of the Union Health policies and procedures including those outlined in this plan. All workforce members who become aware of a disclosure of PHI that is not in compliance with these Union Health policies or this Plan must immediately contact the Privacy Officer so that they may take the necessary steps to mitigate harm to the patient.

G. Retaliatory Actions and Waiver of Rights

Union Health does not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise of their rights, filing a complaint, participating in an investigation, or opposing any act or practice made unlawful under HIPAA regulations as long as the individual is acting on a good faith belief that the opposed is unlawful, and the manner of the opposition is reasonable and does not involve the disclosure of PHI. Union Health may not require individuals to waive their rights as a condition of the provision of treatment, payment, or the enrollment of eligibility for benefits.

H. Policies and Procedures

Union Health has implemented policies and procedures that are designed to comply with the standards, implementation specifications, or other requirements stated under HIPAA or any other federal and state laws. These policies are reasonably designed, taking into account the size and type of activities undertaken by Union Health, to ensure such compliance.

Union Health shall make any changes to its policies and procedures at any time, provided that these changes are documented, and the implementation does not materially affect the content of the Notice of Privacy

Practices. Union Health shall change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation under HIPAA and any other applicable federal and state laws. In the event of changes to the privacy practices stated in the Notices of Privacy Practices and any corresponding policies and procedures, they shall be effective on the date of said change as long as a statement reserving the right to make changes to privacy practices is found in the Notice of Privacy Practices.

IV. ACCESS, USE, AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

A. Definition of Access, Use, and Disclosure

The terms "access," "use," and "disclosure" are defined as follows:

Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Disclosure means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

B. Permitted Uses and Disclosures

Union Health will not use or disclose PHI except as what is permitted, required, or authorized under HIPAA. Permitted uses and disclosures include:

(1) To the individual;
(2) For treatment, payment, or health care operations ("TPO");
(3) Incident to a use or disclosure otherwise permitted or required under HIPAA;
(4) With a valid HIPAA authorization; and
(5) When an opportunity to agree or object is provided.

C. Use and Disclosure by a Business Associate

A business associate may only use and disclose PHI as permitted or required by its business associate agreement or other arrangement, or as required by law. A business associate may not use or disclose PHI in a manner that would violate HIPAA if done by Union Health. A business associate is required to disclose PHI when requested by the Secretary, Union Health, or the individual when the disclosure is to satisfy obligations under HIPAA.

D. Authorization Required

Outside of the permitted or required uses of PHI, Union Health will not use and disclose PHI without a valid HIPAA authorization.

E. Requiring the Opportunity to Object

Union Health may, when required and subject to TPO and other exceptions as described below, use or disclose PHI, provided that the individual is informed in advance of the use and disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure. Union Health may orally inform the individual and obtain the individual's oral agreement or objection to the use or disclosure. Union Health will provide the individual with an opportunity to agree or object to using and disclosing PHI in the Union Health facility directory; to those involved in the individual's care such as a family member, other relative, or a close personal friend; or for notification purposes such as disaster relief efforts.

F. Not Requiring the Opportunity to Object

Uses and disclosure for which an authorization or opportunity to agree or object is not required, PHI may be disclosed without written authorization and when specific requirements are satisfied. These permitted disclosures are:

(1) Required by law;

(2) For public health activities;

(3) About victims of abuse, neglect, or domestic violence;

(4) For health oversight activities;

(5) For judicial and administrative proceedings;

(6) For law enforcement purposes under;

(7) About decedents;

(8) For cadaveric organ, eye or tissue donation purposes;

(9) For research purposes;

(10) To avert a serious threat to health or safety;

(11) For specialized government functions; and

(12) For workers' compensation.

G. De-identified Information

Union Health may use and disclose de-identified PHI without consequence. Information that is de-identified does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual. PHI is deidentified in two (2) different ways:

(1) Determined by a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable; or

(2) Removing the following eighteen identifiers of the individual or of relatives, employers, or household members of the individual:

a. Names;

b. All geographic subdivisions smaller than a State;

c. All elements of dates (except year) for dates directly related to an individual;

d. Telephone numbers;

e. Fax numbers;

f. Electronic mail addresses;

g. Social security numbers;

h. Medical record numbers;

i. Health plan beneficiary numbers;

j. Account numbers;

k. Certificate/license numbers;

l. Vehicle identifiers and serial numbers;

m. Device identifiers and serial numbers;

n. Web Universal Resource Locators (URLs);

o. Internet Protocol (IP) address numbers;

p. Biometric identifiers;

q. Full-face photographic images and any comparable images; and

r. Any other unique identifying number, characteristic, or code; and

Union Health does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the subject of the information.

H. Minimum Necessary Standard

Union Health makes reasonable efforts to limit the PHI to the minimum information necessary to accomplish the intended purpose or use of the disclosure or request. The Minimum Necessary Standard does not apply to the following uses and disclosures:

(1) To healthcare providers for treatment purposes;

(2) To the individual;

(3) With a valid HIPAA authorization;

(4) To the Secretary of Health and Human Services (HHS);

(5) That is required by law; and

(6) That is de-identified.

When using or disclosing PHI to a business associate or providers for auditing purposes, the Minimum Necessary Standard does apply. Other disclosures must be reviewed by the Privacy Officer to ensure that the amount of information being disclosed is the minimum necessary to satisfy the purpose of the disclosure.

I. Marketing and Research

Marketing. Marketing is a means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. Union Health will obtain authorization for any use or disclosure of PHI for marketing unless the communication is directly to the individual or is a promotional gift of nominal value.

Research. HIPAA establishes the conditions under which PHI may be used or disclosed for research purposes. Research is defined as a systematic investigation, including research development, testing, and evaluation designed to develop or contribute to generalized knowledge. Union Health may use or disclose PHI for research with individual authorization, or without it under limited circumstances. Without an individual's authorization, one of the following requirements will be met:

(1) An alteration to or waiver of the individual authorization containing approval by an Institutional Review Board (IRB) or a Privacy Board has been obtained.

(2) It is preparatory to research, which means:

   a. The use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes in preparatory research;

b. No PHI is removed from Union Health; and

c. The PHI for which the use or access is sought is necessary for research purposes.

(3) The individual is deceased, and the researcher provides:

a. Representation that the use or disclosure sought is solely for research on the PHI of decedents;

b. Documentation of the death of such individuals; and

c. Representation that the PHI for which the use or disclosure is sought is necessary for research purposes.

(4) It is used or disclosed under a limited data set as outlined in a data use agreement.

J. Electronic Health Records (EHR)

Union Health's electronic health records comply with HIPAA and other federal and state laws. Union Health has implemented policies and procedures to ensure that all workforce members have appropriate access to PHI in order to prevent those workforce members who do not have access from obtaining access to PHI. Union Health has procedures for the authorization and/or supervision of workforce members who work with PHI or in locations where it may be accessed; to determine that access of a workforce member to PHI is appropriate; and for terminating access to PHI when the employment of a workforce member ends.

K. Access Limitations

Union Health's workforce's access to PHI is limited to the minimum necessary to perform their job responsibilities and what is based on their job description. The workforce shall not use or disclose PHI without a valid HIPAA authorization, or the use or disclosure is otherwise permitted by this Plan and approved under HIPAA. A technical safeguard such as audit controls requires Union Health to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use PHI. An administrative safeguard is an information system activity review where policies and procedures are implemented for a regular review of access audit logs, access reports, and security incident tracking reports. Regular access audits will be run upon request, as part of an investigation, for auditing purposes, or at any time deemed necessary by the Privacy Officer. These audits will be run, reviewed, and documented by the Privacy Officer.

It is a Union Health policy that members of the workforce may not access PHI, in any medium, for themselves, their spouse, their child(ren), their parent(s), or any individual(s) outside the scope of performing their job responsibilities. In the exceedingly rare event that a workforce member must access one of these individuals to perform their job responsibilities, the situation must immediately be reported to their designated leader or the Privacy Officer. There are no shortcuts allowed. Workforce members shall

go through the same procedures as individuals who are not provided access to Union Health PHI. For example, workforce members may not ask their co-workers to look up information for them unless that is their co-worker's responsibility to do so.

L. Removing PHI from Premises

When Union Health determines it is acceptable for a workforce member to work from a location other than a Union Health facility, PHI may be accessed and/or removed only under the following conditions:

- No PHI shall be removed unless approval is received from the Privacy Officer or the Security Officer.
- Paper records shall not be removed unless secured in a secure lock box.
- Union Health shall provide the appropriate equipment for those who are required to work offsite and access PHI.
- Any employee approved to work outside of a Union Health facility must adhere to the following:
    - Only work with PHI in a secure and secluded location.
    - When in transit, PHI must always be kept with you.
    - Those who are not entitled to the PHI must not have access to it.
    - Do not save any PHI or Union Health business information on your home device.
    - Do not print any PHI or Union Health business information.
    - Do not store any login information on or near your device.
    - Return all PHI and business information to the appropriate Union Health facility as soon as possible.

M. Record Retention

The Privacy Officer has established and continually monitors a records retention policy that complies with federal and state requirements. The Privacy Officer will segregate records documenting Union Health's compliance-related obligations. In addition, the Privacy Officer, with the assistance of the Security Officer who oversees the electronic records, will retain records substantially affecting the obligations of Union Health, determine consistent standards for destruction of records to address any allegations of intentional document destruction, monitor and enforce the preservation of documents as required in litigation, institute policies for magnetic or electronic record storage, and to enforce policies for ensuring confidentiality of both personnel and patient records.

V. INDIVIDUAL PRIVACY RIGHTS

A. Notice of Privacy Practices

The Privacy Officer is responsible for developing and maintaining the Union Health Notice of Privacy Practices. An individual has a right to adequate notice of the uses and disclosures of PHI made by Union Health and of the individual rights and legal obligations. This notice is written in plain language and contains the required elements as stated under this regulation. Union Health will ensure this notice is delivered and a written acknowledgment is received by all patients no later than the date of first service delivery, or in an emergency, as soon as reasonably practicable. This notice will be prominently posted in the areas of registration, available upon request for individuals to take with them, and found on the Union Health website. Any material revisions require Union Health to ensure the delivery of the notice by once again, obtaining a written acknowledgment from individuals no later than the first service delivery after the revision.

B. Restrictions

An individual has the right to request a restriction on the uses and disclosures of his/her PHI. It is Union Health's policy to attempt to honor reasonable requests. Union Health will agree to an individual's request to restrict the disclosure of PHI to a health plan if (i) the purpose of the disclosure is to carry out treatment or health care operations and (ii) the PHI pertains solely to the health care item or service for which the individual has paid for the item or service in full. Individuals requesting a restriction to the disclosure of PHI should be directed to the Privacy Officer for a Union Health Request for Restrictions form. The Privacy Officer will facilitate and maintain the documentation of all requests.

C. Confidential Communications

An individual has the right to receive confidential communications. Union Health shall accommodate reasonable requests for individuals to receive communications of PHI by alternative means or to an alternative location. The Privacy Officer has the responsibility of processing requests for confidential communications and working with the necessary departments/offices in order to carry out an approved request.

D. Access

An individual has the right of access to inspect and obtain a copy of PHI contained within the designated record set (the group of medical and billing records, or other records used to make decisions about the individuals), for as long as the PHI is maintained in the designated record set. This right to access excludes psychotherapy notes, SUD counseling notes, and information compiled in reasonable anticipation of, or for

use in, a civil, criminal, or administrative action or proceeding. The individual shall be provided the requested PHI in their preferred format, if readily producible in that format, or if not, in a readable hard copy format as agreed to by Union Health and the individual. All requests for PHI will be directed to the Medical Records Department unless otherwise approved by the Privacy Officer. Requests to inspect PHI will be directed to the Privacy Officer who shall work with the applicable areas to set up a time and place for the inspection.

E. Amendments

An individual has the right to amend their PHI maintained in the designated record set for as long as the PHI is maintained in the designated record set. This request must be submitted in writing and provide a reason which supports the requested amendment. Union Health will respond to the individual's request for an amendment no later than 60 days after the receipt of the request. If this request is not completed within 60 days, an extension of 30 days may be requested by Union Health. Individuals requesting an amendment to their PHI should be directed to the Privacy Officer for a Request for Amendment of Medical Record form. The Privacy Officer will facilitate and maintain the documentation of all requests.

If this request is accepted, Union Health will make the appropriate amendment to the PHI or record, at a minimum, identifying the records that are affected by the amendment and appending, or otherwise providing a link to the location of the amendment. A reasonable effort will be made within an acceptable amount of time to inform and provide the amendment to persons identified on the request. Both an approval and a denial require a response to the individual in writing. The individual will be provided with the opportunity to submit a statement of disagreement in the event their request is denied.

F. Accounting of Disclosures

An individual has the right to receive an accounting of disclosures of PHI made by Union Health going back six (6) years prior to the request. A request for an accounting of disclosure excludes disclosures:

- To carry out treatment, payment, or healthcare operations;
- To individuals of PHI about them;
- Incident to a use or disclosure which are permitted or required under HIPAA;
- When there is a valid HIPAA authorization;
- Included in the Union Health directory or to persons involved in the individual's care or other notification purposes;
- For national security or intelligence;
- To a correctional institution or law enforcement official; or
- That is part of a limited data set.

The accounting of disclosure will contain the date of the disclosure, the name of who received the PHI, if available, the address of who received the PHI, a brief description of the PHI disclosed, and a brief statement of the purpose of the disclosure that reasonably informs the individual of the bases for the disclosure or a copy of the request for the disclosure.

Union Health will respond to a request for an accounting of disclosures within 60 days. An extension of thirty additional days may be requested provided that it presents the individual with notice of the reason for the delay and an expected date of completion. Individuals requesting an accounting of disclosures should be directed to the Privacy Officer for a Request for Accounting of Disclosures form. The Privacy Officer will facilitate and maintain the documentation of all requests.

VI. BREACH OF UNSECURED PROTECTED HEALTH INFORMATION REPORTING

A. Breach Reporting

A breach is defined as the unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of the PHI. The Privacy Officer is responsible for the investigation and attempt to resolve all reported privacy breaches, and the Security Officer is responsible for the investigation and attempt to resolve all reported cybersecurity breaches. Workforce members shall report any event that is believed to be a breach of PHI immediately. This report can be made to the Privacy Officer or the workforce member's leadership. The Privacy Officer will document all privacy and security incidents as well as any corrective actions taken. All documentation of such privacy and security incidents shall retained for six (6) years. Any breach of PHI constitutes a disclosure for which an accounting is required.

Members of the workforce who neglect to report known privacy or security incidents promptly may be subject to disciplinary action.

B. Notification to Individuals

Following the discovery of a breach of unsecured PHI, Union Health shall notify each individual that their unsecured PHI has been, or is reasonably believed to have been accessed, acquired, used, or disclosed as a result of such breach. This notification will be in plain language and provided without reasonable delay and in no case later than sixty calendar days after the discovery of the breach. The individual notice shall be in writing by first-class mail, or if the individual agrees, electronic notice. If Union Health has insufficient or out-of-date contact information for ten or more individuals, Union Health shall provide a substitute notice by posting the notice on its website or posting the notice in major print or broadcast media in geographic areas where the individuals affected by the breach may reside. If Union Health has insufficient or out-of-

date information for fewer than ten individuals, the substitute notice may be provided by an alternative form of written notice, telephone, or other means.

Each notification, to the extent possible, will contain a brief description of what happened; a description of the types of affected unsecured PHI; the steps individuals should take to protect themselves; a brief description of what Union Health is doing to investigate the breach, mitigate harm, and protect against further breaches; and contact procedures to field questions which includes a toll-free telephone number, an email address, website or postal address.

C. Notification to the Media

A breach of unsecured PHI involving more than 500 residents of a state or jurisdiction, Union Health will notify prominent media outlets serving the state or jurisdiction. This media notification will be provided without reasonable delay and no later than 60 days following the discovery of the breach and should include the same information as the individual notices.

D. Notification to the Secretary

The Secretary of Health and Human Services will be notified in the event of a breach of unsecured PHI that affects 500 or more individuals. The notification will be done without reasonable delay, and no later than 60 days following the discovery of the breach. If the breach affects less than five hundred individuals, the notification will be done on an annual basis and no later than 60 days after the end of each calendar year.

E. Notification by Business Associate

A business associate of Union Health shall, following the discovery of a breach of unsecured PHI, notify Union Health of such breach. The business associate shall provide notification without reasonable delay and in no case later than 60 calendar days after the discovery of a breach. To the extent possible, the notification from the business associate shall include the identification of each affected individual who has been or is reasonably believed to have been accessed, acquired, used, or disclosed during the breach. Additionally, the business associate must provide any additional information necessary for Union Health to fulfill its reporting requirements.

F. Incident Response Team

The Privacy Officer and Security Officer are members of the Union Health Incident Response Team. This team is responsible for providing in-depth analysis and recommendations for an appropriate response to breaches that may cause significant harm to individuals or Union Health.

VII. BUSINESS ASSOCIATES

A. Definition

A business associate is an entity that, on behalf of Union Health, but other than in the capacity of a member of the workforce:

- Creates, receives, maintains, or transmits PHI for a function or activity including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and repricing; or
- Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for Union Health, where the provision of service involves the disclosure of PHI from Union Health or other business associate of Union Health to the person.

The following are examples of a business associate:

- A third-party administrator that assists a health plan with claims processing;
- A CPA firm whose accounting services to a health care provider involve access to PHI;
- An attorney whose legal services to a health plan involve access to PHI;
- A consultant who performs utilization reviews for a hospital;
- A healthcare clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a healthcare provider and forwards the processed transaction to a payer;
- An independent medical transcriptionist who provides transcription services to a physician; and
- A pharmacy benefits manager who manages a health plan's pharmacist network.

B. Use and Disclosure

A business associate may use or disclose PHI as permitted or required by its business associate contract or other arrangement, or as required by law. The business associate may not use or disclose PHI in a manner that would violate HIPAA, if done by the covered entity, or violate the terms of the business associate contract or other assurance.

With approval from the Privacy Officer and in compliance with HIPAA, Union Health may disclose PHI to a business associate and allow that business associate to create, receive, maintain, or transmit PHI on its behalf. Before disclosing PHI to a business associate, Union Health will obtain satisfactory assurances that the business associate will implement safeguards as required under HIPAA. Satisfactory assurances will be in the form of a written contract or other written agreement or arrangement with the business associate.

C. Business Associate Agreements or Other Arrangements

A contract or other agreement must meet several requirements. A contract between Union Health and a business associate will contain several different elements including language that establishes permitted and required uses and disclosures of PHI by the business associate and ensures that the business associate will not use or further disclose the PHI other than as permitted or required by the contract or as required by law, report any use or disclosure of PHI not provided for by its contract of which it becomes aware, including breaches of unsecured PHI, and authorize the termination of the contract by Union Health in the event the business associate has violated a material term of the contract.

VIII. GOVERNANCE AND OVERSIGHT

A. Board Oversight.

The Union Health System, Inc. and Union Hospital, Inc. Boards of Directors (collectively, the "Boards") have adopted this Plan by resolution. The Boards will also approve any changes to this Plan.

The Board further authorizes the development, implementation, and ongoing operation of both the Cybersecurity Committee and the Artificial Intelligence (AI) Subcommittee, as described in the following sections. The Boards grant these committees the authority necessary to carry out their responsibilities under this Plan and to support Union Health's overall HIPAA Privacy and Security compliance efforts.

B. Cybersecurity Committee

The Cybersecurity Committee is responsible for governing and overseeing all aspects of Union Health's cybersecurity program to ensure the protection of ePHI and compliance with the HIPAA Security Rule, CISA, and other applicable regulations. This multidisciplinary committee develops and maintains cybersecurity policies and standards, reviews emerging threats and vulnerabilities, and ensures appropriate administrative, technical, and physical safeguards are implemented. It coordinates closely with the Privacy Officer and Security Officer to align cybersecurity efforts with broader organizational risk management objectives. The committee also reviews results of risk analyses, penetration tests, and security audits; tracks mitigation efforts; and makes recommendations to leadership regarding technology investments, training priorities, and incident response preparedness.

C. Artificial Intelligence (AI) Subcommittee

The AI Subcommittee operates under the Cybersecurity Committee to evaluate, govern, and monitor Union Health's use of artificial intelligence and machine learning technologies that may access, process, or generate PHI or other sensitive data. Primary responsibilities of this subcommittee may include: confirming AI applications comply with HIPAA, Part 2, and other applicable privacy and security regulations; promoting ethical, secure, and transparent AI adoption; assessing proposed AI tools for data protection risks; and developing internal standards for responsible AI use and coworker education. The AI Subcommittee reports its findings and recommendations to the Cybersecurity Committee, ensuring that emerging technologies strengthen, rather than compromise, the organization's compliance posture and patient trust.

IX. CODE OF CONDUCT

Union Health's Code of Ethical Conduct is incorporated herein. As shown in the Code of Ethical Conduct attachment, violations may result in disciplinary action, including termination, prosecution, or both.

X. REVISIONS

Document Change Control

Version	Release Date	Summary of Changes	Issuer	Signature
Version 1.0	October 24, 2024	Initial Release	HIPAA Compliance and Privacy Officer	Candie Cuffle
Version 2.0	November 20, 2025	Addition:42 CFR Part 2, CISA, Cybersecurity Committee, and AI Subcommittee Removal: Reproductive Healthcare Information Protections	HIPAA Compliance and Privacy Officer	Candie Cuffle