Chimes International, Ltd., and related entities

PRIVACY COMPLIANCE MANUAL

Privacy Official: Toya Carter
Security Official: Brian Johnson
Issued: October 1, 2019
Last Revised: January 15, 2026

Table of Contents

INTRODUCTION

Chimes International, Ltd., Holcomb Associates, Inc., (also referred to as Chimes Behavioral Health Systems) Chimes, The Chimes, Inc., Chimes Metro Inc., Chimes Virginia, Inc., Family Focus, LLC, Career Support Systems, LLC, and related entities, are subsidiaries and related entities of Chimes International and are members of the Chimes Family of Services (collectively referred to as Chimes), are "covered entities" as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). From time to time, some of these entities may also act at "business associates" as defined by HIPAA. In addition to being a covered entity under HIPAA, some of these entities are also "part 2 programs" under 42 CFR Part 2 ("Part 2").

Chimes takes privacy very seriously. This Privacy Compliance Manual and the Information Security Manual (together, the "Program") are designed to provide a comprehensive system for protecting the confidentiality and security of personal information and to meet the obligations applicable under the HIPAA Privacy Rule, Security Rule, and Breach Notification Rule; Part 2; as well as applicable state law. The Program dictates how Chimes will use, disclose, and protect protected health information ("PHI") in accordance with the terms of the HIPAA Privacy Rule, Security Rule, and Breach Notification Rule. Chimes also provides services on behalf of various counties or other organizations, and subject to various contracts. These contracts may include requirements that are not reflected in this Program. Chimes considers and addresses these contractual obligations on a case-by-case basis.

All members of the workforce who have access to PHI must comply with the Program. For purposes of the Program, the "workforce" includes individuals who would be considered part of the workforce under HIPAA, such as employees, volunteers, interns, board members, and other persons whose work performance is under the direct control of Chimes, whether or not they are paid by Chimes. As used herein, the term "employee" or "staff member" includes all of these types of workers.

Chimes expects all members of its workforce to review and understand the materials contained herein. We welcome any questions or concerns you may have and encourage open dialogue to resolve any issues or concerns.

LEGAL OVERVIEW

I. Federal Law – HIPAA

A. Administrative Simplification

In 1996, Congress passed the Health Insurance Portability and Accountability Act ("HIPAA" or the "Act"). The principal purpose of the legislation was to prevent health care fraud and to provide continuity of health insurance for workers who change jobs. As a part of the same legislation, an "Administrative Simplification" provision was added to address electronic health care transactions.[1]

Placing individual information where it can be accessed electronically, however, also heightens the risk of unauthorized intrusion into files containing personal information that many people consider private. Thus, the push to electronic health care transactions was accompanied by mandates that health care providers, health plans, and clearinghouses (referred to as "covered entities") adopt security protections and privacy procedures to protect the confidentiality, integrity, and availability of that information. The HIPAA Privacy and Security Rules[2] are the two principal sets of regulations under HIPAA with which a covered entity must comply when handling member information. In addition, companies must also consider a variety of state laws designed to protect individuals relative to data breaches, which could compromise personal information.

B. Descriptions and Definitions

Protected Health Information. "Protected health information," or "PHI,"[3] means information transmitted or maintained in any form or medium (including information transmitted orally) that meets all of the following conditions:

(i) is created or received by a health care provider, health plan, employer, or health care clearinghouse;

(ii) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and

(iii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Covered Entity. "Covered Entity"[4] means a health plan, health care clearinghouse, or a health care provider conducting certain standard electronic transactions.

Business Associate. "Business Associate" generally includes any person or entity that creates, receives, maintains, or transmits protected health information on behalf of a covered entity

[1] Public Law 104-191
[2] 45 CFR Parts 160 and 164.
[3] *Id*.
[4] 45 CFR § 160.103.

for a function or activity regulated by HIPAA, including but not limited to, claims processing or administration, data analysis, utilization review, quality assurance, billing, and benefit management.[5] Business Associates may also perform legal, actuarial, accounting, consulting, or any other administrative functions on behalf of the covered entity.[6] It also includes any subcontractor to such a person or entity that provides services involving possession of or access to PHI.[7]

Use; Disclosure. The Privacy Rule and Security Rule apply to the "use" or "disclosure" of PHI. "Use" refers to how the PHI is handled within the entity that maintains it.[8] "Disclosure" refers to any release of PHI outside of the entity that maintains it.[9] The Privacy Rule applies to uses or disclosures regardless of the form in which the information occurs, be it paper, electronic, or oral, while the Security Rule only applies to electronic PHI.

Designated Record Set. "Designated Record Set" means a group of records maintained by or for a covered entity that is: (i) the medical records and billing records about individuals maintained by or for a covered health care provider; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for the covered entity to make decisions about individuals. The term "record" means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity. The Designated Record Set does not include any information compiled in reasonable anticipation, or for use in a civil, criminal, or administrative action or proceeding, including, but not limited to, any information subject to the attorney-client privilege, trial preparation immunity, attorney work product, or other privilege under applicable law.

C. Privacy Rule

The Standards for Privacy of Individually Identifiable Health Information (the "HIPAA Privacy Rule") establishes national standards for the protection of certain individually identifiable information. The HIPAA Privacy Rule permits a covered entity to use or disclose protected health information of an individual for treatment, payment, or health care operations purposes.[10] To meet its obligations, Chimes has performed a variety of activities, including: workforce training on this Program; creating sanctions and disciplinary procedures for employees who violate this Program or HIPAA; and mitigating damages known to have resulted from the improper use or disclosure of PHI. In implementing reasonable safeguards, Chimes has analyzed its own needs and circumstances.

[5] 45 CFR § 160.103.
[6] *Id.*
[7] 45 CFR § 164.502(e)(1)(i).
[8] 45 CFR § 164.504(f)(3).
[9] *Id.*
[10] 45 CFR § 164.506.

1. Administrative Requirements

Privacy Official. Chimes has designated a "Privacy Official" who is responsible for developing and implementing its privacy policies and procedures. The Privacy Official shall serve as the contact person responsible for receiving complaints or inquiries relating to privacy issues.

Training. Chimes has a training program for its workforce regarding the appropriate HIPAA policies and procedures so that they may carry out their jobs in compliance with HIPAA. New employees who will be required to handle or may be responsible for handling PHI are also to be trained within a reasonable period of time after commencement of employment. The Program calls for all training to be documented, and such documentation is to be maintained by the official having responsibility for human resources in accordance with applicable retention policies. The Program calls for all employees with access to PHI to be trained as soon as possible.

Security Safeguards related to the Privacy Rule. Chimes has established appropriate administrative, technical, and physical safeguards to protect the privacy of the PHI that it maintains, if any. In implementing reasonable safeguards, as provided under HIPAA, Chimes has analyzed its particular needs and circumstances.

Complaints, Sanctions, and Mitigation. Any complaints or concerns regarding the privacy or security of PHI maintained by Chimes are directed to the Privacy Official. The Program calls for all such complaints and their disposition to be documented and maintained by the Privacy Official. Chimes has implemented a complaints and non-retaliation Policy to ensure open communication regarding privacy and security concerns and to ensure that an individual may exercise his or her rights under the Privacy Rule, including filing a complaint without fear of retaliation by Chimes. Chimes also has implemented a sanctions policy regarding employees who fail to comply with the Program or the Privacy Rule. Chimes acknowledges its responsibility and obligation to mitigate, to the extent it can, improper uses or disclosures of PHI.

Policies and Procedures. Chimes has implemented reasonable and appropriate policies and procedures through this Program. Chimes will review this Program no less than every two (2) years and upon significant changes or events, and it will update the Program as needed to reflect changes in the law or in the operations of Chimes. Chimes also will amend the Program as necessary if and when there are changes to HIPAA or any other state or federal law regarding personal information that apply to Chimes. The Privacy Official, in consultation with legal counsel to Chimes, as appropriate, is responsible for the continued compliance of the Program with federal and state law.

Retention Period for Documents Related to the Program. All documentation of the Program and actions taken under the Program's policies and procedures are held in accordance with Chimes' retention policies for at least six (6) years from the date of the document's creation or the date it was last in effect, whichever is later.[11] Other state and federal statutes and regulations, however, may call for retention periods longer than six (6) years, in which case compliance with the longer period may be necessary. The Privacy Official, in consultation with legal counsel to Chimes as appropriate, is responsible for determining any such longer retention periods.

[11] 45 CFR § 164.530(j)(2).

2. Use or Disclosure of Protected Health Information

Regulatory Permission. The HIPAA Privacy Rule permits a covered entity to use or disclose PHI of an individual for treatment, payment, or health care operations purposes without the need to have the individual's authorization.

The "Minimum Necessary" Standard. The HIPAA Privacy Rule requires Chimes to make reasonable efforts to limit use and disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose.[12] The Privacy Rule requires that, to the extent practicable, the minimum necessary PHI consists of a "limited data set." The minimum necessary standard is a reasonableness standard, and the Privacy Official uses an approach consistent with best practices and guidelines.

Business Associates. The Privacy Rule permits covered entities to use business associates, and business associates may utilize subcontractor business associates, to carry out functions involving possession of or access to PHI. In the context of these relationships, Chimes must comply with certain requirements. In particular, before Chimes discloses PHI to a business associate, it will enter into a written business associate agreement with the business associate that complies with the requirements under HIPAA.[13] Chimes will maintain copies of all business associate agreements and related service agreements into which it enters.

3. Individual Rights of Individuals

Individuals have certain rights as prescribed by the HIPAA Privacy Rule. These rights broadly stated, include the right to access their Designated Record Set (DRS), the right to restrict access to PHI, the right to an accounting of where the PHI has been disclosed (excluding disclosures for treatment, payment, or health care operations), and the right to amend their DRS. Chimes responds directly to individuals with regard to these rights.

D. Security Rule

The Security Rule standards protect PHI when it is maintained or transmitted electronically (ePHI). The Security Rule requires that covered entities establish procedures and mechanisms to protect the confidentiality, integrity and availability of ePHI. Covered entities must implement administrative, physical and technical safeguards to protect ePHI.[14] Subsequent to the HITECH Act, business associates likewise must have such safeguards in place, and all business associate agreements entered into by Chimes and its business associates require this as well.

Chimes has performed a security risk assessment to identify its compliance with administrative, technical, and physical safeguards. The risk assessment is maintained by the Security Official. Chimes has adopted a separate Information Security Manual to comply with the requirements imposed by the Security Rule.

---

[12] 45 CFR § 164.502(b).
[13] 45 CFR §§ 164.314(a)(2)(i); 164.502(e)(2); and 164.504(e).
[14] 45 CFR § 164.306(a).

E. Breach Notification Rule

The HIPAA regulations were amended in 2009 to include a data breach notification requirement. The Breach Notification Rule was further amended in 2013. Under the regulations, Chimes must provide notification upon the occurrence of a "breach" of "unsecured" PHI. Chimes may be required to notify individuals, the Secretary of the U.S. Department of Health & Human Services, and in some cases the media. HIPAA defines a breach generally as the unauthorized access, acquisition, use, or disclosure of PHI.

HIPAA's Breach Notification Rule also provides an important exception that does not require these notifications if the data in question was appropriately encrypted. The breach notification requirements apply only to "unsecured" PHI, which the Breach Notification Rule essentially defines as PHI that has not been encrypted to NIST standards.

The HIPAA's Breach Notification Rule also provides certain other limited exceptions to what constitutes a "breach," so legal counsel to Chimes should be consulted in any case if an unauthorized access, acquisition, use, or disclosure of PHI is suspected.

II. Federal Law – Part 2

Part 2 protects the privacy and security of "any information (including information on referral and intake) about patients receiving diagnosis, treatment, or referral for treatment for a substance use disorder created by a part 2 program."[15] The term "substance use disorder" is specifically defined as "a cluster of cognitive, behavioral, and physiological symptoms indicating that the individual continues using the substance despite significant substance-related problems such as impaired control, social impairment, risky use, and pharmacological tolerance and withdrawal."[16] However, for purposes of Part 2 the "definition does not include tobacco or caffeine use."[17]

The protections afforded by Part 2 are more stringent than those imposed by HIPAA. For example, with certain exceptions, an authorization is generally required for disclosures of information protected by Part 2.[18] Moreover, a third-party service provider must qualify as a "qualified service organization" before it can receive the protected information it needs to provide services to Chimes.[19]

III. State Law

[15] 42 CFR § 2.12(e). 42 USC § 290dd-2 provides for the confidentiality of all "records of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any program or activity relating to substance abuse education, prevention, training, treatment, rehabilitation, or research, which is conducted, regulated, or directly or indirectly assisted by any department or agency of the United States." 42 USC § 290dd-2(a).
[16] 42 CFR § 2.11.
[17] 42 CFR § 2.11.
[18] 42 CFR § 2.13; 42 CFR § 2.31; 42 CFR § 2.33(a)
[19] 42 CFR § 2.11; 42 CFR § 2.12(c).

Chimes must abide by both federal and state laws regarding the privacy and security of PHI. This can present challenges, as the laws of each state may protect different types of personal information.

A. State Preemption under HIPAA

Delaware, Maryland, New Jersey, Virginia and Pennsylvania maintain numerous state laws addressing the use and disclosure of PHI. The HIPAA regulations have two main rules relating to how they intersect with state law. First, state laws that are contrary to the HIPAA regulations are preempted by HIPAA, which means that the HIPAA regulations control in the event of such a conflict.[20] Second, when a state law is more stringent than the HIPAA regulations, a covered entity or business associate must abide by the more stringent regulation or statute. Thus, Chimes must evaluate the relevant laws of every state applicable to its business and abide by the stricter state laws when applicable.

B. State Data Breach Laws

In addition, every state has enacted its own data breach laws that impact any unauthorized disclosure of personally identifiable information by Chimes (not necessarily limited to health information). If there is a potential breach involving personal information, but the incident does not meet the definition of unsecured protected health information under HIPAA, the incident still must be evaluated for notification requirements under applicable state laws. Conversely, if there is a breach under HIPAA, there still must be a review to determine if state law obligations must also be met. While a majority of affected individuals will likely be from Delaware, Maryland, New Jersey, Virginia or Pennsylvania, the laws applicable to individuals from other jurisdictions should also be reviewed. In all instances, notification will be made in accordance with Chimes' "Data Incident Response and Breach Notification" policy.

[20] 45 CFR § 164.306(a).

PRIVACY
POLICIES AND PROCEDURES

Chimes Privacy Policies & Procedures	
Title: Privacy Policies and Procedures	**No. P001**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes maintains Privacy Policies and Procedures as part of its Compliance Program with respect to patient rights regarding their personal information. Chimes updates the Privacy Policies and Procedures as necessary and appropriate to account for changes in operations and legal obligations. It is Chimes' policy to review these policies on a regular basis, but no less than every other year.

PROCEDURES

I. Privacy Policies & Procedures

A. Chimes maintains Privacy Policies and Procedures setting forth the safeguards and processes to be applied and followed by workforce members in connection with Protected Health Information (PHI). The policies and procedures are reasonably designed, taking into consideration the size and type of Chimes' activities that relate to PHI.

1. A member of the workforce includes any employee, contractor, volunteer, trainee, or other persons whose conduct, in the performance of work for Chimes, is under the direct control of Chimes.

B. The Privacy Official, with input from the Security Official, is responsible for developing and updating privacy policies and procedures. They will review each of the standards identified in the HIPAA Privacy, Security, and Breach Notification Rules, determine how Chimes will comply with each standard, develop policies and procedures that meet the requirements, and document these efforts.

C. All workforce members are provided ongoing access to Chimes' Privacy Policies and Procedures, either electronically or on paper.

D. Workforce members are required to comply with Chimes' Privacy Policies and Procedures.

E. The Privacy Official is responsible for providing or coordinating the training of workforce members on the Privacy Policies and Procedures. Please see Chimes' "Workforce Training, Monitoring, and Sanctions" policy (P003).

II. Routine Review and Revisions

A. The Privacy Official shall routinely review and update Chimes' Privacy Policies and Procedures in response to environmental or organizational changes that affect current operations and applicable changes in laws. The review will usually be conducted in the third quarter of each calendar year.

1. If Chimes revises a privacy policy and procedure that is described in its Notice of Privacy Practices, the change may be effective for PHI that Chimes created or received prior to the revision, if Chimes has included a statement reserving the right to make such a change in the Notice.

2. Chimes may change a privacy policy and procedure that does not materially affect the content of its Notice of Privacy Practices, provided that:

   i. The policy or procedure, as revised, complies with HIPAA;

   ii. The policy or procedure is documented prior to the effective date; and

   iii. Chimes revises the Notice of Privacy Practices and makes the revised notice available as required by Chimes' "Notice of Privacy Practices" policy (P017). Chimes may not implement a change to a policy or procedure prior to the effective date of the revised Notice of Privacy Practices.

3. When there is a change in applicable law that requires a revision to Chimes' policies or procedures, the Privacy Official will promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the Notice of Privacy Practices, the Privacy Official will promptly revise the Notice of Privacy Practices in accordance with Chimes' "Notice of Privacy Practices" policy (P017).

4. When implementing a policy or procedure change to comply with changes in the law, the Privacy Official shall:

   i. Ensure that the policy and procedure complies with the law;

   ii. Document the policy or procedure, as revised; and

   iii. Revise the Notice of Privacy Practices, as appropriate.

B. The Privacy Official shall communicate any material changes to the Privacy Policies and Procedures to workforce members and provide training to affected workforce members.

C. Material revisions to the Privacy Policies and Procedures shall be approved by the Privacy Official, in consultation with the Security Official if necessary.

III. Documentation

A. The Privacy Official will maintain an electronic or hard copy file of the current and archived policies and procedures for at least six (6) years. Paper records may be securely destroyed after the retention period. Electronic records may be deleted, and all backup storage will be erased and destroyed once they no longer need to be retained.

B. Chimes will permit an agent of the Secretary of HHS to access facilities, books, records, accounts, and other information during normal business hours in response to a compliance audit or complaint investigation. If at any time HHS requests access to any facility or books and records, the Privacy Official and legal counsel will be contacted immediately.

REGULATORY REFERENCES

45 CFR § 164.530(i)
45 CFR § 164.530(j)

Chimes Privacy Policies & Procedures	
Title: Privacy Official	**No. P002**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes shall, at all times, have a Privacy Official to oversee and implement its Privacy Program and to ensure Chimes' compliance with applicable privacy requirements, including but not limited to the HIPAA Privacy Rule and state laws governing the privacy of personal information. The Privacy Official shall be responsible for the development and implementation of all privacy policies and procedures for Chimes and for implementing the procedures below. The Privacy Official is also responsible for receiving and responding to complaints about matters of privacy.

From time to time, Chimes may receive requests to provide certain additional privacy protections or to exercise certain individual rights. The Privacy Official will oversee Chimes' policy to timely respond to such requests with careful consideration and respect.

Chimes' Privacy Official is Toya Carter.

PROCEDURES

I. Appointment – Chimes' Board of Directors has appointed a Privacy Official who is principally responsible for the development and implementation of the policies and procedures relating to privacy, including but not limited to this Manual. The assignment and designation of the Privacy Official shall be documented and such documentation shall be maintained for a minimum of six (6) years.

II. Responsibilities - The responsibilities of the Privacy Official include the items listed below. The Privacy Official may delegate any such duties when appropriate, but will maintain oversight over his or her duties. The Privacy Official will be responsible for overseeing implementation and compliance with this Program.

A. Privacy Policies & Procedures

1. Coordinate and assist in development and implementation of policies and procedures to safeguard PHI.

2. Communicate and implement the privacy policies and procedures.

3. Revise the compliance program, including this Manual, to comply with any changes in operations or changes in law.

B. Training

1. Oversee the initial and ongoing training on the Privacy Program for all workforce members who support Chimes' operations. Please see Chimes' "Workforce Training, Monitoring, and Sanctions" policy (P003).

2. Initiate, facilitate, and promote activities to foster privacy information awareness within the organization.

C. Mitigation

1. To the extent practicable, mitigate any known harmful effect that is caused by the use or disclosure of PHI in violation of Chimes' policies and procedures or applicable law. To comply with this obligation, the Privacy Official will coordinate with and require business associates to mitigate, to the extent possible, harmful effects from Breaches of PHI known to them.

2. Develop and implement any corrective actions needed in response to privacy incidents or breaches, in coordination with Human Resources and, as appropriate, the Security Official.

D. Complaints

1. Serve as the individual, along with the Security Official, to receive and investigate complaints regarding privacy. Please see Chimes' "Complaints, Investigations, and Non-Retaliation" policy (P004).

2. Ensure that complaints and their dispositions are documented.

3. Ensure that no intimidation, threats, coercion, discrimination, or any retaliatory actions are taken against any individual for exercising an individual right or filing a complaint.

E. Sanctions

1. In conjunction with the appropriate supervisor/manager, ensure that violations of the Privacy Program and any associated policies and procedures are addressed. Please see Chimes' "Workforce Training, Monitoring, and Sanctions" policy (P003).

2. Document any sanctions that are applied. Copies of sanction documentation shall be retained by Human Resources in the workforce member's personnel file.

F. Work with the Security Official should there be any breach of unsecured PHI that may require notification.

G. Coordinate any responses to complaints or compliance reviews for governmental or accrediting organizations concerning Chimes' compliance with state or federal privacy laws or regulations.

H. Oversee individual rights to inspect, amend, and restrict access to PHI when appropriate, in coordination with Chimes' management.

I. Maintain current knowledge of applicable federal and state privacy and security laws, regulations and sub-regulatory guidance.

J. Administrative Responsibilities

1. Document, in writing, the actions taken in compliance with the HIPAA Privacy Rule and applicable state law.

2. Periodically assess administrative, technical and physical safeguards and update these safeguards as needed.

3. Coordinate with the Security Official, Human Resources and others to ensure that workforce members' access to PHI is terminated as quickly as possible and without undue delay upon cessation of employment, contract, or other arrangement/relationship. This includes ensuring that (a) access is terminated with respect to electronic and hard copy PHI maintained on or within Chimes' systems; and (b) the applicable business associates are notified that the individual is no longer a member of Chimes' workforce.

4. The Privacy Official shall be responsible for securing business associate agreements, when necessary.

III. Documentation. Chimes will maintain a written record of the names and titles of the individuals who serve as the Privacy Official. Such documentation is maintained in written or electronic form for six (6) years.

REGULATORY REFERENCES

45 CFR § 164.530(a)

Chimes Privacy Policies & Procedures	
Title: Workforce Training, Monitoring, and Sanctions	**No. P003**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

In recognition of the paramount importance of the privacy and security of Protected Health Information (PHI), every member of Chimes ' workforce must abide by this Program. Any violation of the Program or associated policies and procedures by a member of the workforce will be grounds for disciplinary action up to and including termination of employment or contract.

PROCEDURES

I. Workforce Training

A. All members of Chimes' workforce who have access to PHI will receive training on Chimes' privacy and security policies and procedures within the first thirty (30) days of their hiring or onboarding and prior to handling any PHI. The Privacy Official shall ensure that workforce members are timely trained.

1. Workforce members will also receive follow-up training at least once annually.

2. Workforce members shall receive regular privacy awareness updates and training.

3. The Privacy Official and Human Resources will document the time, date, place and content of each training session, as well as the workforce members who attended each training session. The Privacy Official and/or Human Resources will take attendance at such trainings to ensure that all workforce members have received training.

B. The Privacy Official shall ensure that Chimes' training program includes:

1. Awareness on privacy, security, and breach notification;

2. An overview of HIPAA, as has been provided above;

3. Protection from, guarding against, and reporting of malicious software;

4. Procedures for creation and protection of passwords; and

5. Any other federal or state privacy, security, and data breach law as the Privacy Official shall deem appropriate.

C. The training shall be tailored to the individual's scope of employment or work, although most workforce members shall generally have similar, if not the same, training needs.

D. The Privacy Official shall ensure that training on any new or modified policies or procedures is provided to workforce members within a reasonable period of time.

E. Training shall be documented by the Privacy Official, in coordination with Human Resources, and retained, with a copy of the documentation in each individual's Human Resources file, or in the case of an independent contractor, in their contract file. The Privacy Official is responsible for ensuring training and Human Resources shall retain the training documentation.

II. Monitoring

A. Limited Access. Only workforce members who need access to PHI to perform their job functions will be granted access to PHI. Workforce members with access to PHI may use and disclose PHI as required for their job, but the PHI disclosed must be limited to the minimum amount necessary to perform the job function and in accordance with Chimes' "Minimum Necessary" policy (P010).

B. Any workforce member who knows or has reason to believe that another person has violated the law or this Program should report the matter promptly to his or her supervisor, the Privacy Official, or the Security Official.

1. All reported matters and complaints shall be investigated and, where appropriate, steps will be taken to remedy the situation.

2. Reports shall be made and investigated in accordance with Chimes' "Complaints, Investigations, and Non-Retaliation" policy (P004).

3. In accordance with Chimes' "Complaints, Investigations, and Non-Retaliation" policy (P004), any attempt to retaliate against a person for reporting a violation of the Program will itself be considered a violation of this policy that may result in disciplinary action up to and including termination of employment or contract with Chimes. Chimes shall not intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against any individual for voicing a concern or complaint.

III. Sanctions

A. Chimes will impose sanctions against any workforce member who violates its privacy and security policies and procedures and applicable law. Chimes reserves the right to impose sanctions as it deems appropriate, and any violation may result in termination of employment or relationship with Chimes.

B. In making the determination of which sanction to impose, Chimes will consider, among other things, the nature and scope of the violation, whether it is a repeat offense, and the workforce member's response to the violation.

C. The Privacy Official shall make recommendations to Human Resources regarding the sanctions for violations of the Program and may utilize the Sanctions Example Matrix below as a basis for making sanctions recommendations.

D. Human Resources, in collaboration with the Privacy Official and, as necessary, the appropriate manager and legal counsel, will make the final determination regarding the appropriate sanctions, taking into account the Privacy Official's recommendations and the written documentation regarding the incident.

E. The Privacy Official and Human Resources shall document any sanctions applied and such documentation shall be retained, with a copy of the documentation in each individual's Human Resources file, or in the case of an independent contractor, in their contract file.

Sanctions Example Matrix

Level and Definition of Incident	***Example of Incident***	***Potential Action***
Accidental and/or due to lack of clarity	• Improper disposal of PHI • Improper protection of records, e.g., leaving PHI unattended on desk, unsecured PC, etc. • Misdirected email, sending email with PHI unencrypted • Misdial fax number • Improper disclosure without properly executed release • (First offenses)	• Re-training and re-evaluation • Oral warning with documented discussion of policy, procedures, and requirements • Termination
Purposeful violation of privacy (purposefully accessing PHI without a legitimate use) or an unacceptable number of previous incidents	• Snooping/Accessing or using PHI without having legitimate need to do so • Not forwarding appropriate information or requests to the Privacy Official for processing, investigation and resolution	• Re-training and re-evaluation • Written warning with documented discussion of policy, procedures and requirements • Termination
Purposeful violation of privacy policy with	• Intentional disclosure of PHI to unauthorized individual or company	• Termination

associated potential individual harm	• Sale of PHI to any source • Any uses or disclosures that could invoke harm to a Workforce Member, individual, or other party	
Multiple Incidents	• Repeated occurrence of any of the above examples or other incidents	• Any sanction described above up to and including termination

REGULATORY REFERENCES

45 CFR § 164.308(a)(1)(ii)(C)
45 CFR § 164.530(b)
45 CFR § 164.530(e)(1)

Chimes Privacy Policies & Procedures	
Title: Complaints and Investigations, and Non-Retaliation	**No. P004**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes shall accept, investigate, and resolve inquiries, complaints and investigations pertaining to the confidentiality and safeguarding of the Protected Health Information of individuals. Chimes will review and resolve complaints regarding suspected violations of Chimes' policies and procedures for maintaining the privacy and security of PHI and other confidential company information.

PROCEDURES

I. Administration

A. The Privacy Official and the Security Official are responsible for creating a system for handling any complaints regarding Chimes' privacy and security practices and for responding to any complaints lodged.

II. Inquiries, Complaints, and Internal Investigations

A. Anyone who knows or has reason to believe that another person has violated applicable law or this Program should report the matter promptly to his or her supervisor (if a member of Chimes' workforce) or to the Privacy Official or the Security Official.

1. Any complaints regarding Chimes' privacy practices shall be directed to the Privacy Official or his or her designee. The Privacy Official shall investigate and respond to all such complaints.

2. Any complaints about Chimes' security practices shall be directed to the Security Official or his or her designee. The Security Official shall investigate and respond to all such complaints in conjunction with the Privacy Official.

B. Any complaints, whether they are from an individual, personal representative, family member, third party, workforce member, or investigative authority (*e.g.*, Office for Civil Rights) should be sent as quickly as possible to the Privacy Official or the Security Official.

1. Chimes recognizes that complaints and alleged violations of privacy or security rights may be forwarded through multiple channels, such as telephone calls, letter via mail/email, in person. If these complaints are received by a workforce member, the person receiving the complaint will:

i. *In response to a telephone call or in-person request to file a complaint*: Immediately forward to the Privacy Official.

ii. *In response to a letter or email*: Immediately forward them to the Privacy Official. Attach the written complaint or a printed copy of the email to the complaint form.

iii. *In response to an anonymous complaint*: Complete the complaint form based on the information provided and immediately forward to the Privacy Official. When possible, explain to the complainant that the Privacy Official will follow up on complaints whether or not they are anonymously filed.

2. Complaints should be requested to be memorialized in writing whenever possible.

3. Workforce members may also report concerns and complaints via the Ethics/Compliance Hotline, which is available to all workforce members at 1-866-384-4277or email to compliance@chimes.org.

C. All reported matters and complaints shall be investigated and, where appropriate, steps will be taken to remedy the situation.

1. Upon receiving an inquiry or complaint regarding privacy or security practices, the Privacy Official or the Security Official, or their designee reviews and addresses the inquiry or complaint as expeditiously as possible given the circumstances or within the time allowed by the inquiry or complaint.

2. All complaints will be initially reviewed by the Privacy Official, or designee to determine if the complaint alleges a violation of established policies and procedures or other known regulations regarding the protection of PHI.

i. During the initial review, the Privacy Official or Security Official, or their designee will:

a. Document the patient's name, Medicare/Medicaid/Private Payor ID number, dates of service, address; and the date the complaint was received;

b. Review the complaint and document the review in NAVEX or its functional equivalent;

c. Advise appropriate workforce members of the complaint and coordinate with them on the review and resolution of the complaint; and

d. Determine whether there is a legitimate allegation. If there is no legitimate allegation, the Privacy Official will, when possible, contact the complainant by letter and inform him/her of this finding within sixty (60) days.

3. If there is a legitimate allegation, the Privacy Official, or designee will conduct a detailed investigation by reviewing all relevant information and by working with the Security Official, or designee (as applicable).

i. In conducting their investigations, the Privacy Official or the Security Official, or their designee will:

a. Review and investigate the complaint and document the review/investigation;

b. Advise appropriate workforce members of the complaint and coordinate with them on the review and resolution of the complaint; and

c. Document the resolution.

ii. Where possible, Chimes shall make every effort to handle the reported matter confidentially.

D. Upon conclusion of the investigation, the Privacy Official or the Security Official or their designee shall:

1. Prepare a written report with findings and conclusions to present to the appropriate members of the management team.

2. In conjunction with management and legal counsel, make the final determination regarding the appropriate action based upon the written report.

i. Sanctions will be imposed against any workforce member who violates the Program in accordance with Chimes' "Workforce Training, Monitoring, and Sanctions" policy (P003).

3. Contact the complainant by letter and inform him/her of the finding within sixty (60) days and document that the complainant was so advised.

4. Retain complaint records for a minimum of six (6) years.

E. Mitigation. In the event that an inquiry or complaint reveals a use or disclosure of PHI that is in violation of Chimes' Policies and Procedures or the law, Chimes shall mitigate, to the extent practicable, any harmful effect of the impermissible use or disclosure. Please see Chimes' "Mitigation" policy (P016)

III. Refraining From Intimidation or Retaliatory Acts

A. Chimes and its workforce members will refrain from intimidating, threatening, coercing, discriminating against, or taking any retaliatory action against any person for the exercise of a right established by, or for participation in any process provided under, HIPAA, including, without limitation:

1. voicing a concern or filing a complaint;

2. testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing involving a HIPAA compliance issue; or

3. opposing any act or practice made unlawful by HIPAA, provided that the person has a good faith belief that the practice opposed is unlawful, that the manner of opposition is reasonable, and that the person does not unlawfully disclose PHI.

B. Any attempt to retaliate against a person for reporting a potential violation of law or the Program will itself be considered a violation of this policy that may result in disciplinary action up to and including termination of employment or contract with Chimes.

C. Chimes will not require any person to waive his or her rights to file a complaint or his or her rights under the Privacy, Security, or Breach Notification Rules, as a condition of treatment.

IV. External Investigations

A. Chimes shall cooperate with an investigation of Chimes' privacy practices that may be undertaken by the United States Department of Health and Human Services.

1. Correspondence, notices of investigation or complaints from the U.S. Department of Health & Human Services, Office for Civil Rights, or other enforcement authority, shall promptly and without delay be sent to the Privacy Official, who will coordinate the response.

2. The Privacy Official shall coordinate the response to the investigation in consultation with other executives as well as legal counsel, as appropriate.

B. The Privacy Official, in consultation with legal counsel, reviews and responds as expeditiously as possible given the circumstances, or within the time allowed if the complaint is received in connection with an investigation by Chimes' privacy practices by the United States Department of Health and Human Services.

REGULATORY REFERENCES

45 CFR § 164.530(d)(1)
45 CFR § 164.530(d)(2)
45 CFR § 164.530(g)

45 CFR § 164.530(h)

Chimes Privacy Policies & Procedures	
Title: Technical, Physical, and Administrative Safeguards	**No. P005**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes will use appropriate administrative, physical and technical safeguards to protect the privacy of Protected Health Information (PHI) from an intentional or unintentional use or disclosure that is in violation of HIPAA and/or Chimes' contractual obligations. Chimes also uses reasonable safeguards to limit incidental uses or disclosures made as part of an otherwise permitted or required use or disclosure. The PHI that is to be safeguarded may be in the form of oral, electronic, or paper communications. PHI may be found in both paper and electronic form.

Chimes has also implemented its "Additional Safeguards for Part 2 Programs" policy (P006).

PROCEDURES

I. General Procedures

A. The Privacy Official shall ensure that Chimes implements and uses appropriate administrative, technical, and physical safeguards to protect the privacy of PHI. The Privacy Official shall determine the operational risk areas for unauthorized uses and disclosures of PHI and put reasonable safeguards in place to mitigate the risks.

B. The Privacy Official and the Security Official will periodically assess and update the safeguard procedures established by this Policy as necessary to conform to operational changes or changes in applicable law.

II. Specific Safeguards

A. Physical Safeguards

1. *Use, Storage, and Destruction of Paper Information*

i. Chimes has implemented a "clean desk" policy. All non-electronic PHI shall be secured each time a workforce member is away from his/her desk. No PHI shall be left on a workforce member's desk while he or she is away from his/her desk for an extended period of time, and desks must be cleared of materials containing PHI at the end of the business day.

ii. Personnel with access to PHI shall be designated and all incoming documentation will be directed to such personnel, generally either through US mail or interoffice mail.

iii. Any paper documents containing PHI must be placed in locked files, locked desk drawers, or designated record rooms with locked doors. All such drawers, cabinets, and rooms are to be locked and are only accessible to authorized personnel. Such drawers, cabinets, and rooms shall not be accessible to the public.

iv. Where paper copies of PHI are outside of storage for use, they will be placed in folders, under a coversheet, face down on a working surface, or handled in a similar manner to prevent unintended access to such PHI.

v. Material containing PHI must be promptly removed from faxes, printers and photocopiers.

vi. PHI in paper format will be destroyed by shredding when no longer needed. All papers containing PHI to be discarded must be placed in the shred bin, which is to be emptied on an as-needed basis.

2. *Facsimiles*

i. Any facsimile machines are maintained in secure environments and are not kept where they can be accessed by the public.

ii. PHI will not be left on a fax machine unattended. Once a fax is sent or received, the documentation will promptly be removed.

iii. Fax numbers shall be checked to ensure correctness and all faxing must be made carefully and with appropriate cover sheets. A facsimile transmittal sheet that does not contain PHI will be used when sending any fax that contains PHI.

3. *Oral Conversations*

i. All oral conversations concerning PHI shall be limited in content in conformance with Chimes' "Minimum Necessary" policy (P010).

ii. All conversations involving PHI shall be held only with authorized individuals. Please see Chimes' "Verification" policy (P009).

iii. Workforce members are not allowed to discuss an individual's PHI in public places such as hallways, kitchens and bathrooms.

iv. Workforce members must take reasonable steps to protect the privacy of verbal discussions of PHI that take place at workstations. If a conversation cannot reasonably be made private and not overhead, workforce members shall refrain from holding the conversation until it can be moved to a secure location (except in

emergencies when treatment of the patient requires immediate communication).

v. Speaker phone should not be used unless in an office with a closed door.

vi. Workforce members should refrain from including PHI in voicemail messages.

B. Technical Safeguards

1. Where electronic copies of PHI are maintained by Chimes, access to such information will be limited to those workforce members who require access to perform their job duties. Electronic PHI will be maintained in accordance with Chimes' Information Security Policies.

i. If necessary to save electronic files containing PHI, such files must be saved to secured folders. Files temporarily downloaded to computers should be deleted immediately after use.

ii. Employees must lock computer screens when away from desks in remote or off-site locations.

iii. Employees must clear PHI from the computer screen when not actually being used.

iv. Computer passwords are to be made as strong as possible, kept confidential and not be shared with others, written down or otherwise disclosed to others.

2. *Text Messages*

i. Workforce members should not generally utilize text messages, including SMS, MMS, and iMessage transmissions, for work purposes. If a text message is used, it may not include PHI.

ii. Chimes may utilize an application that provides secure texting; however, it is generally not the preferred manner of communication.

3. *Email*

i. All PHI in emails sent within Chimes' information systems shall be limited in conformance with Chimes' "Minimum Necessary" policy (P010). (e.g., workforce members shall refrain from forwarding string emails containing PHI, instead creating new messages that limit the PHI and the recipients of the email).

ii. Emails containing PHI sent over the internet shall be limited and shall be encrypted by including "secure" in the subject line of the email.

iii. Emails containing any work information or PHI shall never be sent from a personal email address by any workforce member. Where a patient requests information, including PHI, to be sent to a patient's personal email, Chimes must have permission.

iv. Workforce members are not permitted to forward or otherwise transmit work information or PHI to the workforce member's personal email account. Where workforce members are authorized to work from home or off-site, workforce members must utilize their Chimes email address to send and receive such information.

v. Workforce members may only access the email system after a password entry.

vi. Any faxes routed to workforce members through Chimes' email system and shall be handled in accordance with policies related to email use.

vii. The use of smart voice technology (e.g., Amazon Alexa and Echo, Google Home, Apple Siri, etc.) in Chimes facilities and resident rooms is not permitted. The technology and devices connect, engage, and exchange data, and may pose significant cybersecurity and privacy concerns.

C. Administrative Safeguards.

1. The Privacy Official will make reasonable efforts to limit the access of workforce members identified as needing access to PHI.

2. All workforce members will undergo training on the Program.

3. Workforce members will make reasonable efforts to limit uses and disclosures of PHI to the minimum necessary to accomplish the intended purpose of the use or disclosure in accordance with Chimes' "Minimum Necessary" policy (P010).

4. Workforce members shall report to the Privacy Official any use and disclosure such workforce member believes to be unlawful. The Privacy Official shall investigate and resolve any wrongful uses and disclosures. Please see Chimes' "Complaints, Investigations, and Non-Retaliation" policy (P004).

III. Privacy Official Review

A. The Privacy Official will periodically assess and update the safeguard procedures established by this Policy.

REGULATORY REFERENCES

45 CFR § 164.530(c)

Chimes Behavioral Health Systems Privacy Policies & Procedures	
Title: Additional Safeguards for Part 2 Programs	**No. P006**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes protects the confidentiality of information identifying individuals as having a substance use disorder. This policy is adopted to ensure Chimes' compliance with the additional safeguards and controls required by 42 CFR Part 2.

PROCEDURES

I. The Privacy Official shall ensure that Chimes implements and uses appropriate safeguards to protect the privacy of information identifying individuals as having a substance use disorder, including those additional safeguards required by 42 CFR Part 2. Please see Chimes' "Classification of Information" policy (P011).

II. Identification Cards

A. Chimes shall not require any patient to carry in their immediate possession while away from Chimes' premises any card or other object which would identify the patient as having a substance use disorder.

B. Chimes may require patients to use or carry cards or other identification objects on Chimes' premises.

REGULATORY REFERENCES

42 CFR § 2.17
42 CFR § 2.18
16 CFR § 681.1

Chimes Privacy Policies & Procedures	
Title: Authorizations for Uses and Disclosures	**No. P007**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes relies on signed authorizations from the individual or the individual's authorized representative for all uses and disclosures of Protected Health Information (PHI) beyond those otherwise required or permitted by the Privacy Rule. A separate authorization is required for each person or organization that is to receive the PHI. Chimes shall ensure that an authorization, which is compliant with HIPAA and applicable state laws, has been obtained prior to any use or disclosure of PHI for which an authorization is required.

This policy also outlines the additional requirements that apply when the authorization applies to information identifying an individual as having a substance use disorder. Please see Chimes' "Classification of Information" policy (P011).

PROCEDURES

I. General Procedures

A. All uses and disclosures, other than those permitted by the HIPAA Privacy Rule, require a valid authorization from the individual.

B. Individuals will generally submit any required authorizations for the use and/or disclosure of PHI to Chimes. However, if Chimes is acting as a business associate, the workforce member will work with the client to obtain from the individual a HIPAA-compliant authorization that also meets state law obligations (if any).

C. Workforce members shall ensure that any uses and discloses of PHI made pursuant to an authorization are consistent with the terms of the authorization.

D. Workforce members shall not use an authorization that:

1. has expired;

2. is incomplete or does not include all of the required information;

3. has been revoked;

4. is improperly compound; or

5. is known to be false.

E. An individual may revoke an authorization at any time. The revocation shall be submitted in a writing that specifies the authorization to be revoked. A revocation will be effective immediately unless the individual specifies a future date in his or her written revocation. The revocation will not be valid where Chimes has already acted in reliance upon the authorization.

1. Upon receipt of a revocation, the Privacy Official shall:

i. Date-stamp the notification of revocation;

ii. Record the revocation in the patient's medical record; and

iii. Notify appropriate parties of the revocation.

F. Chimes shall not condition the provision of treatment to an individual on the provision of an authorization.

1. Chimes may condition the provision of research-related treatment on the provision of an authorization for the use or disclosure of PHI for such research.

2. Chimes may condition the provision of treatment that is solely for the purpose of creating PHI for disclosure to a third party on the provision of an authorization for the disclosure of the PHI to such third party if the sole purpose of the treatment is to provide PHI to a third party (*e.g.*, disclosure of the results of an employer-mandated drug test to the employer).

G. Documentation.

1. The Privacy Official or his/her designee is responsible for retaining and documenting any signed authorization received from patients.

i. Chimes will maintain authorization forms on file in accordance with its "Document Retention" policy .

2. The Privacy Official or his/her designee shall ensure that all expiration dates for authorizations are recorded and tracked.

3. If Chimes seeks an authorization for a use or disclosure of PHI, Chimes must provide a copy of the signed authorization form to the individual.

4. *Standard Form*.

i. Chimes has adopted, and its workforce members shall use, the template authorization form approved by the Privacy Official.

ii. Individuals or their authorized representatives are asked to complete Chimes' standard authorization at the time of registration.

H. The Privacy Official may consult with the Corporate Privacy Official and legal counsel as needed in fulfilling his or her obligations under this policy.

II. Review of Authorization

A. If an individual presents to Chimes an authorization other than Chimes' standard form authorization, workforce members shall send such authorization to the Privacy Official for review. The Privacy Official may approve such form, if it contains the required elements identified in Sections B and C below.

B. The Privacy Official, or his or her designee, shall, prior to using or disclosing the member's PHI, ensure that the authorization is written in plain language and includes, at a minimum, the following:

1. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

2. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;

3. The name or other specific identification of the person(s), or class of persons, to whom Chimes may make the requested use or disclosure;

4. A description of each purpose of the requested use or disclosure;

   i. This description must be specific enough to provide an individual with the facts that he/she needs to make an informed decision about whether to allow release of the PHI.

   ii. The statement "at the request of the individual" is a sufficient description of the purpose only when an individual initiates the authorization and does not (or elects not to) provide a statement of the purpose.

5. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;

6. A statement of the individual's right to revoke the authorization in writing and either (a) a statement of the exceptions to the right to revoke and a description of how to revoke; or (b) a reference to a notice of privacy practices, if the notice describes the exceptions to the right to revoke and the revocation process;

7. A statement prohibiting the conditioning of health care on the provision of the authorization;

8. A statement addressing the potential for information disclosed pursuant to the authorization to be re-disclosed by the recipient; and

9. The signature of the individual and the date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

C. In addition to those requirements in Section B above, the following are required as indicated below:

1. If the authorization is for marketing that involves direct or indirect payment from a third party, the authorization from the individual must state that payment is involved in order to be valid.

2. If the authorization is for the sale of PHI, the authorization from the individual must state that payment is involved in order to be valid.

D. Workforce members shall not rely upon an improperly compound authorization.

1. An authorization may not be combined with any other document to create a compound authorization, except as set forth in the exceptions below. Workforce members shall forward any compound authorization to the Privacy Official for review. The Privacy Official, or his or her designee, may only approve a compound authorization if one of the following exceptions applies:

i. An authorization for the use or disclosure of PHI for a research study may be combined with any other type of written permission for the same or another research study. This exception includes combining an authorization for the use or disclosure of PHI for a research study with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research.

ii. An authorization to use or disclose psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.

iii. An authorization covered under this Policy (other than an authorization for a use or disclosure of Psychotherapy Notes) may be combined with any other authorization covered under this Policy, except when Chimes has conditioned the provision of health care on the provision of the authorization.

2. One authorization may be used to send the same information to two recipients. However, if different information is sent to two recipients, two separate authorizations should be obtained.

III. Marketing Communications

A. Chimes shall not use or disclose PHI in connection with marketing communications, as defined by the HIPAA Privacy Rule, without first obtaining a

valid HIPAA authorization from the individual who is the subject of the PHI when required by HIPAA.

B. Prior to commencing any use of PHI that may qualify as "marketing," workforce members shall consult the Privacy Official, who shall consult with the Corporate Privacy Official and legal counsel, as appropriate, to ensure compliance with legal requirements, including assessing whether an authorization is required.

C. The Privacy Official shall review all authorizations for marketing by Chimes to determine whether the authorization is complete and valid.

IV. Sale of PHI. Chimes shall obtain a valid authorization before engaging in any sale of PHI. An authorization for sale of PHI must state that Chimes is receiving payment for the disclosure.

V. Authorizations Involving Substance Use Disorder Information

A. With Authorization. Chimes may typically disclose Substance Use Disorder Information, in accordance with a valid consent and authorization, to any person or category of persons identified or generally designated in the consent.

1. Prior to making any disclosure pursuant to an authorization, Chimes shall review the authorization presented to ensure that it includes the required elements outlined in Subsection B of this Section.

2. Authorizations shall be retained by the Privacy Official in accordance with Chimes' document retention policies.

3. Limitations.

i. Disclosures to central registries and/or withdrawal management or maintenance treatment programs to prevent multiple enrollments must meet special requirements, and the Privacy Official, who may consult with legal counsel, shall be consulted prior to any disclosures.

i. Where state law requires parental consent to treatment, the fact of a minor's application for treatment at Chimes may be communicated to the minor's parent, guardian, or other individual authorized under state law to act in the minor's behalf **only** if:

1. The minor has given written consent to the disclosure; or

2. The minor lacks the capacity to make a rational choice regarding such consent as judged by Chimes' program director.

ii. Expired or Revoked Authorizations.

1. Chimes shall not disclose any Substance Use Disorder Information based on an authorization known to have been revoked.

2. Chimes shall not disclose any Substance Use Disorder Information based on a consent which has expired.

B. Authorization Requirements. A written consent to a disclosure of Substance Use Disorder Information under Part 2 may be in paper or electronic form and must include:

1. The name of the patient;

2. The specific name(s) or general designation(s) of the Part 2 program(s), entity(ies), or individual(s) permitted to make the disclosure;

3. A description of how much and what kind of information is to be disclosed, including an explicit description of the substance use disorder information that may be disclosed;

4. The name(s) of the individual(s) to whom a disclosure is to be made

i. Alternatively, if the recipient entity has a treating provider relationship with the patient whose information is being disclosed (such as a hospital, a health care clinic, or a private practice) the name of that entity shall be included.

ii. Alternatively, if the recipient entity does not have a treating provider relationship with the patient whose information is being disclosed and is a third-party payer, the name of the entity shall be included.

iii. Alternatively, if the recipient entity does not have a treating provider relationship with the patient whose information is being disclosed and is not a payer (such as an entity that facilitates the exchange of health information or a research institution), the consent/authorization shall include the name(s) of the entity(-ies); and

a. The name(s) of an individual participant(s); or

b. The name(s) of an entity participant(s) that has a treating provider relationship with the patient whose information is being disclosed; or

c. A general designation of an individual or entity participant(s) or class of participants that must be limited to a participant(s) who has a treating provider relationship with the patient whose information is being disclosed. However, when using a general designation, a statement must be

included on the consent form that the patient (or other individual authorized to sign in lieu of the patient), confirms their understanding that, upon their request and consistent with this part, they must be provided a list of entities to which their information has been disclosed pursuant to the general designation.

5. The purpose of the disclosure;

6. A statement that the authorization is subject to revocation at any time, except to the extent that Chimes has already acted in reliance on it;

7. The date, event, or condition upon which the consent will expire if not revoked before; provided, however that the date, event, or condition must ensure that the consent will last no longer than reasonably necessary to serve the purpose for which it is provided;

8. The signature of the patient or authorized representative; and

9. The date on which the authorization is signed.

10. Please note, the patient may elect to provide a single authorization for future uses of the Substance Use Disorder treatment records for treatment, payment and healthcare operations, as described in HIPAA, beginning on April 16, 2024 and forward, without the need to execute separate authorizations for each individual recipient of information for these purposes.

11. For treatment, payment and healthcare operation purposes, disclosures of Substance Use Disorder treatment records made according to the above described "single patient authorization" may be made in accordance with the HIPAA Privacy Rule.

C. Who Can Provide the Authorization?

1. *For Incompetent Patients*. If the patient is incompetent, the Privacy Official, who may consult legal counsel, shall be consulted prior to any disclosures to determine the individual authorized to give consent and the additional signature(s) required for the authorization, if any.

   i. *Adjudicated*. In the case of a patient who has been adjudicated as lacking the capacity, for any reason other than insufficient age, to manage their own affairs, consent may be given by the guardian or other individual authorized under state law to act on the patient's behalf.

   ii. *Not Adjudicated*. In the case of a patient, other than a minor or one who has been adjudicated incompetent, that for any period suffers from a medical condition that prevents knowing or effective action

on their own behalf, Chimes' program director may exercise the right of the patient to consent to a disclosure for the **sole** purpose of obtaining payment for services from a third-party payer and no substance abuse or other sensitive information (HIV, STDs pregnancy, etc.) is included.

2. *For Deceased Patients*. If the patient is deceased, the Privacy Official, who may consult with legal counsel, shall be consulted to determine the individual authorized to give consent and the additional signature(s) required for the authorization, if any.

    i. Consent may be given by an executor, administrator, or other personal representative appointed under applicable state law. If there is no such applicable state law appointment, the consent may be given by the patient's spouse or, if none, by any responsible member of the patient's family.

3. *For Minor Patients*. If the patient is a minor, the Privacy Official, who may consult with legal counsel, shall be consulted to determine the individual authorized to give consent and the additional signature(s) required for the authorization, if any.

    i. If state law does not require parental consent to treatment:

        a. If a minor patient acting alone has the legal capacity under the applicable state law to apply for and obtain substance use disorder treatment, any written consent may be given **only** by the minor patient.

            1. This restriction includes, but is not limited to, any disclosure of patient identifying information to the parent or guardian of a minor patient for the purpose of obtaining financial reimbursement, and Chimes will not disclose information to the minor's parents or guardians without authorization.

    ii. If state law requires parental consent to treatment:

        a. Where state law requires consent of a parent, guardian, or other individual for a minor to obtain treatment for a substance use disorder, any written consent must be given by **both** the minor and the parent, guardian, or other individual authorized under state law to act in the minor's behalf.

D. Minimum Necessary. Chimes limits the disclosure of Substance Use Disorder Information to that information which is necessary to carry out the stated purpose.

E. Notice Regarding Re-Disclosure.

1. Every disclosure of Substance Use Disorder Information made with the patient's consent shall be accompanied with a written notice regarding re-disclosure of the Substance Use Disorder Information.

2. The notice shall state either:

i. "42 CFR part 2 prohibits unauthorized use or disclosure of these records."

ii. "This record which has been disclosed to you is protected by Federal confidentiality rules (42 CFR part 2). These rules prohibit you from using or disclosing this record, or testimony that describes the information contained in this record, in any civil, criminal, administrative, or legislative proceedings by any Federal, State, or local authority, against the patient, unless authorized by the consent of the patient, except as provided at 42 CFR 2.12(c)(5) or as authorized by a court in accordance with 42 CFR 2.64 or 2.65. In addition, the Federal rules prohibit you from making any other use or disclosure of this record unless at least one of the following applies: (i) Further use or disclosure is expressly permitted by the written consent of the individual whose information is being disclosed in this record or as otherwise permitted by 42 CFR part 2. (ii) You are a covered entity or business associate and have received the record for treatment, payment, or health care operations, or (iii) You have received the record from a covered entity or business associate as permitted by 45 CFR part 164, subparts A and E. A general authorization for the release of medical or other information is NOT sufficient to meet the required elements of written consent to further use or redisclose the record (see 42 CFR 2.31)."

F. Tracking Disclosures. Chimes logs the following information for each disclosure of Substance Use Disorder Information disclosed within the past three (3) years pursuant to the general designation in an authorization:

1. A list of the entities to which their information was disclosed pursuant to the general designation;

2. The date of each disclosure; and

3. A brief description of the patient identifying information disclosed.

VI. Questions. Any questions regarding whether a use or disclosure pursuant to an authorization is permitted or required by law should be directed to the Privacy Official.

REGULATORY REFERENCES

45 CFR § 164.508(a)(1)
45 CFR § 164.508(a)(3)
45 CFR § 164.508(b)(1)–(2)

45 CFR § 164.508(b)(3)
45 CFR § 164.508(b)(4)
45 CFR § 164.508(b)(6)
45 CFR § 164.508(c)(1)–(4)
42 CFR § 2.1-2.68

Chimes Privacy Policies & Procedures	
Title: Personal Representatives	**No. P008**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes treats an individual's personal representative as the individual with respect to uses and disclosures of the individual's protected health information (PHI), as well as the individual's rights under the Privacy Rule (except as may be otherwise provided in the Privacy Rule).

PROCEDURES

I. General Procedures

A. Chimes and its workforce members shall generally treat an individual's personal representative as the individual.

1. Workforce members must first determine whether the individual is (1) an adult or emancipated minor; (2) an un-emancipated minor; (3) deceased; or (4) a victim of abuse, neglect, or endangerment.

2. After making this determination, workforce members shall follow the procedures for the applicable category, as set forth below.

3. Workforce members shall direct all questions to the Privacy Official, who may consult with legal counsel as appropriate.

II. Recognizing a Personal Representative

A. Adults and Emancipated Minors. If the individual is an adult or emancipated minor, then the personal representative is a person with legal authority to make health care decisions on behalf of the individual. All questions should be directed to the Privacy Official or legal counsel as appropriate.

1. Examples include: a person with health care power of attorney, a court-appointed legal guardian; and a person with general power of attorney.

2. Under Delaware law, a competent adult may give written instructions to an individual or execute a power of attorney for health care. Any advance health-care directive must be in writing, signed by the individual or at his/her direction, dated, and signed by two disinterested witnesses. Delaware has adopted standard optional forms for advance health-care directives. In certain instances, when there is no appointed agent, a surrogate may make a health-care decision for an individual. Workforce members shall consult the Privacy Official prior to treating a surrogate as

an individual's personal representative. (16 Del. C. §§ 2503; 2305; and 2507).

3. Under Maryland law, an advance directive that is signed, dated, and subscribed by two witnesses can be used to name a health care agent. The state has adopted standard forms that can be used for this purpose. In certain instances, when there is no appointed agent, a surrogate may make a health-care decision for an individual. Workforce members shall consult the Privacy Official prior to treating a surrogate as an individual's personal representative. (Md. Code Ann., Health-Gen. §§ 5-602, 5-602.01 and 5-604).

4. New Jersey law recognizes a proxy directive (a durable power of attorney for healthcare) and an instructive directive (a living will). Either must be signed and dated by, or at the direction of, the individual in the presence of either (a) two subscribing adult witnesses, who attest that the declarant is of sound mind and free of duress and undue influence; or (b) a notary public or attorney. (N.J. Stat. Ann. § 26:2H-53, *et seq.*).

5. Pennsylvania recognizes a health care power of attorney, a living will, or a combination of the two as advanced health care directives. Both documents must be dated, signed by the individual or at his/her direction, and witnessed by two individuals. (20 Pa. Stat. and Cons. Stat. Ann. § 5421, *et seq.*).

6. Virginia recognizes a healthcare advanced directive which must be signed dated and subscribed by two witnesses. (Va. Coe. Ann. §§54.1-281 to 54.1-2993.1)

B. Un-emancipated Minors. If the individual is an un-emancipated minor, then the personal representative is a parent, guardian, or other person acting "*in loco parentis*" (that is, a person acting in place of the parents) with legal authority to make health care decisions on behalf of the minor child.

1. *Exception*. Chimes will not treat a person as the minor's personal representative if:

i. The minor consents to the health care service, no other consent is required by law, and the minor has not requested that another person be treated as his/her personal representative; or

ii. The minor may lawfully obtain the health care service without the consent of a parent, guardian, or other person and the minor, a court, or another person authorized by law consents to the health care services; or

iii. The parent, guardian or other person acting *in loco parentis* agrees to an agreement of confidentiality between Chimes and the minor.

2. Under Delaware law, a minor 14 years of age or older may give written consent to a treatment facility for voluntary treatment for nonresidential treatment for a substance use disorder. Likewise, a person between 14 and 18 years of age, who is in need of mental health treatment, may request voluntary outpatient treatment from a licensed treatment facility or community provider. (Del. Code Ann. tit. 16, §§ 2210 & 5003).

3. Under Maryland law a minor has the same capacity as an adult to consent to medical treatment if the minor: (1) is married; (2) is the parent of a child; or (3) is living separate and apart from his/her parent, parents, or guardian, and is self-supporting. In addition, a minor also has the same capacity as an adult to consent to, among others, (1) treatment for or advice about drug abuse and (2) treatment for or advice about alcoholism. However, the capacity to consent to treatment for drug abuse or alcoholism does not include the capacity to refuse treatment for drug abuse or alcoholism in a certified inpatient or intensive outpatient alcohol or drug abuse treatment program for which a parent or guardian has given consent. A minor has the same capacity as an adult to consent to psychological treatment if, in the judgment of the attending physician or a psychologist, the life or health of the minor would be affected adversely by delaying treatment to obtain the consent of another individual. Finally, a minor who is 12 years old or older has the same capacity as an adult to consent to consultation, diagnosis, and treatment of a mental or emotional disorder by a health care provider or a clinic if the minor is determined by a health care provider to be mature and capable of giving informed consent. However, this capacity to consent does not include the capacity to (i) refuse consultation, diagnosis, or treatment for a mental or emotional disorder for which a parent, guardian, or custodian of the minor has given consent; or (ii) if the minor is under the age of 16 years, consent to the use of prescription medications to treat a mental or emotional disorder. (Md. Code Ann., Health-Gen. §§ 20-102 and 20-104).

4. Under New Jersey law, when a minor believes that he or she is adversely affected by a substance use disorder involving drugs or an alcohol use disorder or is a person with a substance use disorder involving drugs or an alcohol use disorder, the minor's consent to treatment under the supervision of a licensed physician (or an individual licensed or certified to provide treatment for an alcohol use disorder, or in a facility licensed to provide for the treatment of an alcohol use disorder), is valid and binding as if the minor had achieved the age of majority.

   When a minor who is 16 years of age or older believes that he or she is in need of behavioral health care services for the treatment of mental illness or emotional disorders, the minor's consent to temporary outpatient treatment, excluding the use or administration of medication, under the supervision of a physician licensed to practice medicine, an advanced practice nurse, or an individual licensed to provide professional counseling (a psychiatrist, licensed practicing psychologist, certified social worker, licensed clinical

social worker, licensed social worker, licensed marriage and family therapist, certified psychoanalyst, or licensed psychologist), or in certain licensed outpatient health care facilities, shall be valid and binding as if the minor had achieved the age of majority. (N.J. Stat. Ann. § 9:17A-4).

5. Under Pennsylvania law, a minor who suffers from the use of a controlled or harmful substance may give consent to furnishing of medical care or counseling related to diagnosis or treatment. (71 Pa. Stat. Ann. § 1690.112). In addition, any minor who is fourteen years of age or older may consent on his or her own behalf to voluntary inpatient mental health treatment or outpatient mental health examination and treatment. (35 Pa. Stat. Ann. § 10101.1). The consent must be in writing and obtained only after the minor receives an explanation of the treatment and his or her rights and demonstrates that he or she substantially understands the nature of the treatment. (50 Pa. Stat. Ann. §§ 7201 & 7203).

6. Under Virginia law, a minor shall be deemed an adult for the purpose of consenting to outpatient care for the treatment of a mental illness or substance abuse. (Va. Code Ann § 54.1-2969)

7. If a minor requests certain protections or restrictions regarding their information, workforce members shall contact the Privacy Official, who may consult with legal counsel, as appropriate.

C. Deceased Persons. If the individual is deceased, then the personal representative is a person with legal authority to act on behalf of the decedent or the estate (not restricted to health care decisions), such as the executor or administrator.

1. Workforce members shall consult the Privacy Official, who may consult legal counsel, in the event of a request for a decedent's PHI.

D. Victims of Abuse, Neglect, or Endangerment. Chimes may elect not to treat a person as an individual's personal representative if (1) the individual has been or may be subjected to domestic violence, abuse, or neglect by such person, or treating such person as the personal representative could endanger the individual; *and* (2) Chimes, in the exercise of professional judgment, determines that it is not in the best interest of the individual to treat the person as the individual's personal representative.

1. Workforce members shall consult the Privacy Official, who may consult legal counsel, in instances of suspected abuse, neglect, or endangerment to determine the appropriate personal representative.

III. Verification of Authority

A. Workforce members shall obtain written documentation of a person's authority to act as the individual's personal representative. Workforce members shall make

reasonable inquiry as to the availability and authority of a personal representative under applicable state law.

B. Verification shall occur pursuant to Chimes' "Verification" policy (P009).

REGULATORY REFERENCES

45 CFR § 164.502(g)
42 CFR § 2.14-2.15

Chimes Privacy Policies & Procedures	
Title: Verification	**No. P009**
Responsible Party: Privacy Official	April 10, 2019 Date: December 1, 2018
Last Reviewed Date: December 5, 2025	Revision History: 12/1/18; 4/10/19; 10/1/19; 5/1/23, 1-15-26

POLICY

Chimes requires any party requesting disclosures of Protected Health Information (PHI) to be verified before any disclosure may take place.

PROCEDURES

I. General Procedure. Workforce members shall take reasonable steps to verify the identity of a party requesting the disclosure of PHI as set forth in this Policy.

A. Unless known by the workforce member, any party requesting the disclosure of PHI must be identified, and the party's authority to receive access to PHI must be verified before any disclosure may take place.

1. However, if Chimes is acting as a business associate, the workforce member shall refer the request to Chimes' covered entity client so that the client may confirm the identity and authority of the requestor. In such instances, Chimes is not responsible for determining the legitimacy or adequacy of the documentation submitted to and maintained by the client, and will not review the documentation to determine compliance with the requirements of the jurisdiction in which it was issued.

B. In the event Chimes is required, under the applicable services agreement, to verify the identity of a party requesting the disclosure of PHI, workforce members shall follow the procedures set forth below.

II. Identification of Persons

A. Individuals

1. If the individual is unknown to Chimes, workforce members may request photo identification, a letter or oral authorization, marriage certificate, birth certificate, enrollment information member identification or claim identification.

2. If the individual is acting as a personal representative, the workforce member shall also ask the individual to present legal documentation supporting an individual's authority as the representative of a deceased person. The documentation shall be reviewed pursuant to Section III below.

3. If the individual is a public official or law enforcement, workforce members shall escalate the matter to the Privacy Official, and the Privacy Official shall obtain agency identification, badge, official credentials, or identification or other proof of government status. The documentation shall be reviewed pursuant to Section III below.

B. Entities (health plans, provider groups, other covered entities, etc.). Workforce members shall request identifying information about the entity (including the entity's name, address, phone number, and/or fax number) and the person making the request (in accordance with Section II.A above).

C. If at any time the workforce member who is verifying the information becomes uncomfortable or suspects that there is an issue, the workforce member shall escalate the verification to the Privacy Official. Workforce members shall also escalate any questions or concerns regarding a person's identity or authority to the Privacy Official. The Privacy Official may legal counsel as necessary.

III. Review of Documentation and Authority

A. When Chimes is presented with documentation that purports to confer authority to act on behalf of another, the receiving workforce member shall carefully review such documentation to ensure it meets the criteria detailed below. Any question should be directed to the Privacy Official, who may consult with legal counsel.

B. Authorizations. The content of an authorization submitted shall be reviewed pursuant to Chimes' "Authorizations for Uses and Disclosures" policy (P007).

C. Guardians/Conservators. Chimes must receive and review a copy of the orders of guardianship or conservatorship evidencing the appointment of the person as the individual's legal guardian or conservator, and any disclosure or release of PHI must be consistent with the scope of the letters presented.

1. *Generally*. Legal guardianships typically terminate when the minor attains the age 18, unless the minor is disabled, in which case the legal guardian will continue to serve in the capacity of a conservator. Chimes will not release or disclose PHI to a legal guardian if the patient is over the age of 18 unless evidence of disability is presented and the Order of Guardianship is presented.

2. *State-specific Requirements*. The Privacy Official, or his or her designee, in conjunction with legal counsel, shall review the orders of guardianship or conservatorship for compliance with applicable state law.

D. Powers of Attorney

1. *General Requirements*.

i. The power of attorney must be in writing, signed by the individual, and either notarized or signed by two witnesses.

ii. Unless otherwise stated in the durable power of attorney for health care or medical power of attorney, a person appointed as a durable power of attorney for health care is considered a designated representative of the individual. Please see Chimes' "Personal Representative" policy (P008).

iii. *Effect of Divorce, Dissolution or Annulment of Marriage, or Legal Separation*. Unless expressly provided in the power of attorney, durable power of attorney for health care, or medical power of attorney, the appointed person's power of attorney or durable power of attorney for health care authority is automatically revoked upon divorce, dissolution of marriage, annulment of marriage, or legal separation between the patient and the appointed person.

iv. *Revocation of Power of Attorney, Durable Power of Attorney for Health Care or Medical Power of Attorney*. The individual may revoke the power of attorney or durable power of attorney for health care at any time. Revocation terminates the power of attorney or durable power of attorney for health care.

v. *Death of the Individual*. Powers of attorney and medical durable powers of attorney terminate with the death of the patient.

2. *State-specific Requirements*. Please see Chimes' "Personal Representative" policy (P008). The Privacy Official, in conjunction with legal counsel, shall review powers of attorney and other advance directives for compliance with applicable state law.

3. *Out-of-State Power of Attorney or Durable Power of Attorney for Health Care*. Workforce members shall direct out-of-state powers of attorney to the Privacy Official, may consult with legal counsel.

E. Executors/Administrators. Chimes must receive a copy of the court order, letters testamentary, and/or letters of administration appointing the person to act as the executor, administrator, or personal representative of the decedent's estate. Deceased persons have privacy rights for fifty (50) years after their deaths, and a person who was an individual's personal representative while that individual was alive is not necessarily the probate personal representative.

F. Public Officials/Law Enforcement.

1. *Verification of Identity for Written Documents*. Workforce members shall forward any written request from a public official or law enforcement to the Privacy Official. The Privacy Official shall verify that the request is on appropriate government letterhead. If the person is acting on behalf of a

public official, the Privacy Official will require a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

2. *Verification of Authority*. Chimes may rely on the following to verify the authority of a public office, if reliance is reasonable under the circumstances:

   i. A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;

   ii. A request made pursuant to legal process (warrant, subpoena, order, summons or other legal process issued by a grand jury or a court) is presumed to constitute legal authority.

   iii. A separate written statement that, on its face, demonstrates that the applicable legal requirements have been met.

G. Legal process (subpoenas). Workforce members shall obtain a copy of the applicable document (warrant, subpoena, order, etc.), and immediately forward a copy to the Privacy Official, who may consult with legal counsel.

H. Research Purposes. Workforce members shall forward requests regarding disclosures for research purposes to the Privacy Official, who shall review the request.

1. *Written Acknowledgment of Requestor*. The Privacy Official may rely on a written acknowledgment of a requestor consistent with applicable research laws and Chimes' research policies and procedures.

2. *Written Statement of Institutional Review Board (IRB)*. The Privacy Official may rely on a written statement regarding alteration or waiver of an authorization which confirms that documentation containing the following information has been obtained:

   i. The statement identifies the IRB and the dates on which the alteration or waiver of authorization was approved;

   ii. The statement provides that the IRB has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:

      a. The use or disclosure of PHI involves no more than minimal risk to individuals participating in the research;

b. The alteration or waiver will not adversely affect the privacy rights and the welfare of the research participants;

c. The research could not practicably be conducted without the alteration or waiver;

d. The research could not practicably be conducted without access to and use of the PHI;

e. The privacy risks to individuals whose PHI is to be used or disclosed are reasonable in relation to the anticipated benefits if any to the individuals, and the importance of the knowledge that may reasonably be expected to result from the research;

f. There is an adequate plan to protect the identifiers from improper use and disclosure;

g. There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers, or such retention is otherwise required by law; and

h. There are adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of PHI would be permitted by the Privacy Rule.

iii. A brief description of the PHI for which use or access has been determined to be necessary by the IRB;

iv. A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review process; and

v. A signature by the chair or other member, as designated by the chair, of the IRB.

IV. Exceptions. The Privacy Official may, in the exercise of professional judgment, approve the following without verification pursuant to the foregoing:

A. Uses and disclosures for involvement in the patient's care (please see Chimes' "Uses and Disclosures of PHI – Treatment, Payment, Health Care Operations" policy (P013.02));

B. Uses and disclosures for notification of the patient's location, general condition, or death (please see Chimes' "Uses and Disclosures of PHI – Persons Involved in Care; Notification; Facility Directory" policy (P013.07));

C. Uses and disclosures for disaster relief (please see Chimes' "Uses and Disclosures of PHI – Public Health" policy (P013.06)); or

D. Disclosures to avert a serious threat to the health or safety of the patient, another person or the public (please see Chimes' "Uses and Disclosures of PHI – Public Health" policy (P013.06)).

REGULATORY REFERENCES

45 CFR § 164.502(f)
45 CFR § 164.514(h)

Chimes Privacy Policies & Procedures	
Title: Minimum Necessary	**No. P010**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019 1, 2018
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Subject to the exceptions below, Chimes makes reasonable efforts to limit the use and disclosure of, and requests for, Protected Health Information (PHI) to the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request. Exceptions to the minimum necessary policy include the following:

- disclosures to or requests by a health care provider for treatment purposes;
- uses or disclosures made to an individual as permitted under the Privacy Rule;
- uses or disclosures made pursuant to a written authorization from an individual;
- disclosures made to the Secretary of HHS for compliance and enforcement purposes;
- uses or disclosures that are required by law; and
- uses and disclosures that are required in order to comply with the HIPAA Privacy Rule.

PROCEDURES

I. Uses and Disclosures of PHI by Chimes

A. When using or disclosing PHI, workforce members will limit the use or disclosure to the minimum amount of PHI necessary to accomplish the intended purpose of the use or disclosure.

1. Responses to requests for the disclosure of PHI will be reviewed on an individual basis consistent with minimum necessary criteria. For all requests for disclosure of PHI, workforce members will make reasonable efforts to determine the identification and authority of the party requesting PHI. Please see Chimes' "Verification" policy (P009).

2. Workforce members shall use reasonable judgment in using and disclosing PHI. Workforce members will only use or disclose an entire medical record when the entire medical record is specifically justified as being reasonably necessary to accomplish the purpose of the use or disclosure.

3. Workforce members shall consult the Privacy Official prior to using or disclosing any information regarding substance use disorders, mental health, developmental disabilities, or communicable diseases. The Privacy Official will only approve any such use or disclosure as permitted by state and federal law.

4. When the intended purpose of the use or disclosure can be achieved without information that identifies the patient, the PHI used or disclosed should be

limited to a "limited data set." Please see Chimes' "De-Identification of PHI and Limited Data Sets" policy (P013.08).

B. Internal Uses of PHI.

1. The Privacy Official, or his or her designee, will (1) identify the classes of persons in Chimes' workforce who need access to PHI to carry out their duties, and (2) for each category of persons, define the types or amounts of PHI to which access is needed and any conditions appropriate to that access.

2. The Privacy Official will make reasonable efforts to limit the access of the classes of persons identified to the appropriate PHI. Access to PHI in information systems will be limited, to the extent technically possible, to information needed by the workforce members to carry out their respective duties.

3. Managers will also make reasonable efforts to limit the access of workforce members identified as needing access to PHI who are under their supervision. Managers must authorize each person's access to automated information systems.

4. As a part of compliance training, workforce members are educated regarding use of the minimum necessary standard in their daily activities.

C. Routine Disclosures of PHI: For routine disclosures of PHI to third parties, Chimes has implemented policies and procedures that identify the routine disclosures and that limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

D. Non-Routine Disclosures of PHI.

1. For all disclosures not identified as routine, the Privacy Official will review each request for disclosure of PHI received from a third party and determine what PHI is reasonably necessary to accomplish the purpose of the disclosure.

2. The Privacy Official may consider the following factors:

i. The purpose of the use or disclosure;

ii. The identity of the party that would use or disclose the information;

iii. Whether the recipient of the PHI is a covered entity or business associate regulated by HIPAA;

iv. The amount of PHI involved;

v. The nature, extent and sensitivity of the PHI involved;

vi. The risk of financial, reputational or other harm to the individual;

vii. The extent to which PHI can be extracted from a record without undue burden; and

viii. Safeguards to assure the confidentiality of the information.

E. Requests for PHI from Specific Parties. Workforce members may rely, if such reliance is reasonable under the circumstances, on a requested disclosure to be for the minimum amount of PHI necessary for the stated purpose in the following instances:

1. When making disclosures to public health agencies and law enforcement officials if the requesting official represents that the information requested is the minimum necessary for the stated purpose;

2. When the information is requested by another covered entity;

3. When the information is requested by a health care professional (*e.g.*, a physician or nurse) who is a member of Chimess workforce or is a business associate of Chimes for the purpose of providing professional services to Chimes, if the professional represents that the information requested is the minimum necessary for the stated purposes.

4. When the information is requested for research purposes and the person requesting the information has provided documentation or representations; provided that the Privacy Official shall review all requests for PHI requested for research purposes.

II. Requests for PHI by Chimes

A. In requesting PHI from other entities, Chimes will limit the information requested to that which is reasonably necessary to accomplish the purpose for which the request is made.

1. When the intended purpose of the request can be achieved without information that identifies the patient, the PHI requested should be limited to a limited data set.

2. Workforce members will only request an entire medical record when the entire medical record is specifically justified as being reasonably necessary to accomplish the purpose of the request.

3. Non-routine requests. For all non-routine requests, the Privacy Official will review each request and determine what PHI is reasonably necessary to accomplish the purpose of the request:

   i. The Privacy Official may consider the following factors:

      a. The purpose of the use or disclosure;

      b. The identity of the party that would use or disclose the information;

      c. Whether the recipient of the PHI is a covered entity or business associate regulated by HIPAA;

      d. The amount of PHI involved;

      e. The nature, extent and sensitivity of the PHI involved;

      f. The risk of financial, reputational or other harm to the individual;

      g. The extent to which PHI can be extracted from a record without undue burden; and

      h. Safeguards to assure the confidentiality of the information.

III. Questions. Workforce members shall consult with the Privacy Official, should there be any questions regarding uses, disclosures, and requests for PHI or regarding the minimum amount of PHI necessary. The Privacy Official, and legal counsel, if necessary, shall make determinations on a case-by-case basis.

REGULATORY REFERENCES

45 CFR § 164.514(d)(1)-(2)
45 CFR § 164.514(d)(3)
45 CFR § 164.514(d)(4)
45 CFR § 164.514(d)(5)

Chimes Privacy Policies & Procedures	
Title: Classification of Information	**No. P011**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes is committed to protecting the confidentiality of information that identifies individuals as having a substance use disorder and to complying with the protections afforded to such information by 42 CFR Part 2.

Chimes has adopted specific policies and procedures addressing the limited ways in which Substance Use Disorder Information can be used and/or disclosed. Substance Use Disorder Information will only be used and disclosed in accordance with those policies; it will not be used or disclosed under Chimes' general HIPAA policies and procedures.

PROCEDURES

I. Administration

A. Before using or disclosing any information, workforce members must determine whether the information to be used or disclosed is or includes any Substance Use Disorder Information, as defined in Section II of this policy.

B. Workforce members shall consult the Privacy Official, who shall consult with legal counsel as needed, when determining whether information is Substance Use Disorder Information.

C. The Privacy Official shall train the members of the workforce who handle Substance Use Disorder Information regarding this policy.

II. Classification of Information.

A. The following, when created by or on behalf of Chimes or another federally-assisted substance use disorder program, are "Substance Use Disorder Information":

1. All information and records created by Chimes in connection with its treatment for substance use disorders;

2. Any information, whether recorded or not, which would identify an individual as having or having had a substance use disorder;

i. A "**substance use disorder**" includes any cluster of cognitive, behavioral, and physiological symptoms indicating that the individual continues using the substance (drugs or alcohol) despite significant substance-related problems such as impaired control,

social impairment, risky use, and pharmacological tolerance and withdrawal.

ii. Types of information (including information on referral and intake) included:

a. Patient identifying information, such as the person's name, address, social security number, fingerprints, photograph, or similar information by which the individuals' identity can be determined with reasonable accuracy either directly or by reference to other information;

b. Information about an individual's diagnosis, treatment, or referral for treatment for a substance use disorder by Chimes.

c. Information that would directly identify an individual as having or having had a substance use disorder.

d. Information that would, by reference to publicly-available information, identify an individual as having or having had a substance use disorder.

e. Information that would, through verification of such identification by another person, identify an individual as having or having had a substance use disorder.

f. Any record of a diagnosis identifying a patient as having or having had a substance use disorder prepared by Chimes in connection with or for the purposes of treatment or referral for treatment of a patient with a substance use disorder, even if the diagnosis is not ultimately used for those purposes.

iii. Types of individuals included:

a. Current and former patients;

b. Any individual who has applied for or been given diagnosis, treatment, or referral for treatment for a substance use disorder at Chimes, even if not a current or former patient.

c. Any individual who, after arrest on a criminal charge, is identified as an individual with a substance use disorder in order to determine that individual's eligibility to participate in a part 2 program.

3. Drug abuse information obtained by a federally-assisted drug abuse program for the purpose of treating a substance use disorder, making a diagnosis for that treatment, or making a referral for that treatment; and

4. Alcohol abuse information obtained by a federally-assisted alcohol abuse program for the purpose of treating a substance use disorder, making a diagnosis for that treatment, or making a referral for that treatment.

B. The following are **not** "Substance Use Disorder Information," even if they meet the criteria set forth in Section 2 of this policy:

1. Information regarding a diagnosis made solely for the purpose of providing evidence for use by law enforcement agencies or officials; and

2. Information regarding a diagnosis of drug overdose or alcohol intoxication which clearly shows that the individual involved does not have a substance use disorder (e.g., involuntary ingestion of alcohol or drugs or reaction to a prescribed dosage of one or more drugs).

III. Substance Use Disorder Information Records.

A. Patient records containing information determined to be Substance Use Disorder Information shall be physically and/or electronically marked as containing Substance Use Disorder Information.

B. Patient records which do not contain Substance Use Disorder Information may be used and disclosed in accordance with Chimes' HIPAA policies and procedures; those records are not subject to the Substance Use Disorder Information policies.

C. Patient records containing Substance Use Disorder Information may **only** be used or disclosed in accordance with those policies and procedures applicable to Substance Use Disorder Information.

D. The rights to access and/or to request the amendment of protected health information are not limited by 42 CFR Part 2, and those rights are addressed in Chimes' "Access to PHI" policy (P019) and "Amendment to PHI" policy (P020).

Regulatory References

42 CFR § 2.11
42 CFR § 2.12

Chimes Privacy Policies & Procedures	
Title: Uses and Disclosures of Substance Use Disorder Information - Overview	
	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes is committed to protecting the confidentiality of information that identifies individuals as having a substance use disorder and to complying with the protections afforded to such information by 42 CFR Part 2. Chimes has adopted specific policies and procedures addressing the limited ways in which Substance Use Disorder Information can be used and/or disclosed.

Records which do not contain Substance Use Disorder Information may be used and disclosed in accordance with Holcomb's "Use and Disclosure of PHI" policies.

42 CFR Part 2 is a complex regulation. Should staff have any questions regarding compliance with this regulation, staff should seek guidance from the Privacy Official and or legal counsel.

PROCEDURES

I. Uses and Disclosures

A. Records containing Substance Use Disorder Information may **only** be used or disclosed in accordance with:

1. Holcomb's "Use and Disclosure of Substance Use Disorder Information with an Authorization" policy (P012.01); and

2. Holcomb's "Use and Disclosure of Substance Use Disorder Information without an Authorization" policy (P012.02).

B. Holcomb limits the disclosure of Substance Use Disorder Information to that information which is necessary to carry out the stated purpose. Please see Holcomb's "Minimum Necessary" policy (P010).

C. These Policies limit the use and disclosure of information determined to be "Substance Use Disorder Information" pursuant to Holcomb's "Classification of Information Policy" (P011).

II. The rights to access and/or to request the amendment of protected health information are not limited by 42 CFR Part 2.

REGULATORY REFERENCES

42 CFR § 2.31
42 CFR § 2.32

42 CFR § 2.33
42 CFR § 2.34
42 CFR § 2.35

Chimes Privacy Policies & Procedures	
Title: Uses and Disclosures of Substance Use Disorder Information – With an Authorization	**No. P012.01**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes is committed to protecting the confidentiality of information that identifies individuals as having a substance use disorder and to complying with the additional protections afforded to such information by 42 CFR Part 2.

This Policy limits the use and disclosure of information determined to be "Substance Use Disorder Information" pursuant to Chimes' "Classification of Information Policy" (P011).

PROCEDURES

I. With Authorization. Chimes may typically disclose Substance Use Disorder Information, in accordance with a valid consent and authorization, to any person or category of persons identified or generally designated in the consent.

A. Prior to making a disclosure pursuant to an authorization, Chimes staff shall review the authorization presented to ensure that it includes the required elements outlined in Chimes's "Authorizations Policy" (P007). Any questions related to the authorization should be directed to the Privacy Official.

B. Authorizations shall be retained by Chimes in accordance with Chimes' document retention policies.

1. Please note, the patient may elect to provide a single authorization for future uses of the Substance Use Disorder treatment records for treatment, payment and healthcare operations, as described in HIPAA, beginning on April 16, 2024 and forward, without the need to execute separate authorizations for each individual recipient of information for these purposes.

2. For treatment, payment and healthcare operation purposes, disclosures of Substance Use Disorder treatment records made according to the above described "single patient authorization" may be made in accordance with the HIPAA Privacy Rule.

C. Limitations.

1. Disclosures to central registries and/or withdrawal management or maintenance treatment programs to prevent multiple enrollments must meet special requirements, and the Privacy Official who may consult with legal counsel, shall be consulted prior to any disclosures.

2. Disclosures made in connection with criminal justice referrals must meet special requirements, and the Privacy Official, who may consult with legal counsel, shall be consulted prior to any disclosures.

3. Where state law requires parental consent to treatment, the fact of a minor's application for treatment at Chimes may be communicated to the minor's parent, guardian, or other individual authorized under state law to act in the minor's behalf **only** if:

    i. The minor has given written consent to the disclosure; or

    i. The minor lacks the capacity to make a rational choice regarding such consent as judged by Chimes' program director.

2. Expired or Revoked Authorizations.

    i. Chimes shall not disclose any Substance Use Disorder Information based on an authorization known to have been revoked.

    ii. Chimes shall not disclose any Substance Use Disorder Information based on a consent which has expired.

II. Notice Regarding Re-Disclosure.

A. Every disclosure of Substance Use Disorder Information made with the patient's consent shall be accompanied with a written notice prohibiting re-disclosure of the Substance Use Disorder Information.

B. The notice shall state either:

    i. 42 CFR part 2 prohibits unauthorized use or disclosure of these records."

III. "This record which has been disclosed to you is protected by Federal confidentiality rules (42 CFR part 2). These rules prohibit you from using or disclosing this record, or testimony that describes the information contained in this record, in any civil, criminal, administrative, or legislative proceedings by any Federal, State, or local authority, against the patient, unless authorized by the consent of the patient, except as provided at 42 CFR 2.12(c)(5) or as authorized by a court in accordance with 42 CFR 2.64 or 2.65. In addition, the Federal rules prohibit you from making any other use or disclosure of this record unless at least one of the following applies: (i) Further use or disclosure is expressly permitted by the written consent of the individual whose information is being disclosed in this record or as otherwise permitted by 42 CFR part 2. (ii) You are a covered entity or business associate

and have received the record for treatment, payment, or health care operations, or (iii) You have received the record from a covered entity or business associate as permitted by 45 CFR part 164, subparts A and E. A general authorization for the release of medical or other information is NOT sufficient to meet the required elements of written consent to further use or redisclose the record (see 42 CFR 2.31)**Tracking Disclosures**. The Privacy Official shall ensure that Chimes logs the following information for each disclosure of Substance Use Disorder Information disclosed within the past three (3) years pursuant to a general designation in an authorization:

A. A list of the entities to which their information was disclosed pursuant to the general designation;

B. The date of each disclosure; and

C. A brief description of the patient identifying information disclosed.

REGULATORY REFERENCES

42 CFR § 2.31
42 CFR § 2.32
42 CFR § 2.33
42 CFR § 2.34
42 CFR § 2.35

Chimes Privacy Policies & Procedures	
Title: Uses and Disclosures of Substance Use Disorder Information – Without an Authorization	**No. P012.02**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes is committed to protecting the confidentiality of information that identifies individuals as having a substance use disorder and to complying with the protections afforded to such information by 42 CFR Part 2.

This Policy limits the use and disclosure of information determined to be "Substance Use Disorder Information" pursuant to Chimes' "Classification of Information Policy" (P011).

PROCEDURES

I. Without an Authorization. Chimes is typically prohibited from disclosing Substance Use Disorder Information without a valid authorization.

A. In responding to a request for Substance Use Disorder Information which cannot be disclosed, Chimes will respond in a way that will not affirmatively reveal that an identified individual has been, or is being, diagnosed or treated for a substance use disorder.

B. Chimes will not affirmatively tell the inquiring party that 42 CFR Part 2 restricts the disclosure of the records of an identified patient.

C. The Privacy Official may consult legal counsel when responding to requests.

D. Under Delaware law, personal and medical records shall be treated confidentially and shall not be made public without the consent of the patient, except such records as are needed for a patient's transfer to another health care institution or as required by law or third party payment contract. No personal or medical records shall be released to any person inside or outside Chimes who has no demonstrable need for such records. (16 Del. C. § 2220).

E. Under Pennsylvania law, records may be disclosed only with the patient's consent and only (i) to medical personnel exclusively for purposes of diagnosis and treatment of the patient; (ii) to government or other officials exclusively for the purpose of obtaining benefits due the patient as a result of his drug or alcohol abuse or drug or alcohol dependence, except that in emergency medical situations where the patient's life is in immediate jeopardy, patient records may be released without the patient's consent to proper medical authorities solely for the purpose of providing medical treatment to the patient; (iii) to a covered entity or a covered

entity's business associate that makes the use, disclosure or request for disclosure in accordance with 45 CFR Pt. 164 Subpt. E (relating to privacy of individually identifiable health information). (71 Pa. Stat. Ann. § 1690.108).

II. Limited Exceptions. Without a valid authorization from the individual or an authorized personal representative, Chimes will **only** use or disclose Substance Use Disorder Information as set forth in this policy. Substance Use Disorder Information may not otherwise be disclosed or used in any civil, criminal, administrative, or legislative proceedings conducted by any federal, state, or local authority.

A. Internal Communications. Chimes may communicate Substance Use Disorder Information internally between or among personnel having a need for the information in connection with their duties that arise out of the provision of diagnosis, treatment, or referral for treatment of patients with substance use disorders.

B. Qualified Service Organizations. Chimes may disclose Substance Use Disorder Information to a Qualified Service Organization, so long as the information disclosed is limited to the information needed by the Qualified Service Organization to provide services to Chimes.

1. A Qualified Service Organization includes an individual or entity who:

i. Provides services to Chimes (such as data processing, bill collecting, dosage preparation, laboratory analyses, or legal, accounting, population health management, medical staffing, or other professional services, or services to prevent or treat child abuse or neglect, including training on nutrition and child care and individual and group therapy), and

ii. Has entered into a written agreement with Chimes that:

a. Acknowledges that in receiving, storing, processing, or otherwise dealing with any patient records from Chimes, it is fully bound by the regulations at 42 CFR Part 2; and

b. If necessary, will resist in judicial proceedings any efforts to obtain access to patient identifying information related to substance use disorder diagnosis, treatment, or referral for treatment except as permitted by 42 CFR Part 2.

iii. Please see Chimes' "Business Associates and Qualified Service Organizations" policy (P023).

C. Reporting Crimes. Chimes may disclose Substance Use Disorder Information to law enforcement agencies or officials only as follows:

1. The Substance Use Disorder Information to be disclosed must be:

i. Directly related to a patient's commission of a crime on Chimes' premises or against Chimes' personnel; or

ii. Directly related to a patient's threat to commit a crime on Chimes' premises or against Chimes' personnel.

2. Any use or disclosure of Substance Use Disorder Information for the purposes of reporting a crime must be limited to:

i. The patient status of the individual committing or threatening to commit the crime,

ii. The individual's name and address, and

iii. The individual's last known whereabouts.

3. Discharge dates of patients whose records contain Substance Use Disorder Information may only be disclosed when the requirements set forth above are satisfied. These requirements are more stringent than those set forth in Chimes' "Uses and Disclosures of Substance Use Disorder Information" policies (P012), which applies when the patient's records do not contain Substance Use Disorder Information.

4. Substance Use Disorder Information may not be used to initiate or substantiate any criminal charges against an individual or to conduct any criminal investigation of an individual.

i. Substance Use Disorder Information may not be introduced as evidence in a criminal proceeding or otherwise used to investigate or prosecute a patient with respect to a suspected crime.

ii. This restriction applies to any information obtained by Chimes for the purpose of diagnosis, treatment, or referral for treatment of patients with substance use disorders.

D. Reporting Child Abuse. Chimes may use or disclose Substance Use Disorder Information to report incidents of suspected child abuse and neglect, under state law, to the appropriate state or local authorities.

1. After reporting the child abuse or neglect, Chimes must continue to apply the protections afforded by 42 CFR Part 2 to the original Substance Use Disorder Information, and may not, without an authorization, disclose or use the Substance Use Disorder Information for civil or criminal proceedings which may arise out of the report of suspected child abuse and neglect.

E. Cause of Death Reporting. Chimes may disclose patient identifying information relating to the cause of death of a patient under laws requiring the collection of death or other vital statistics or permitting inquiry into the cause of death.

F. Medical Emergency. Chimes may disclose patient identifying information to medical personnel to the extent necessary to meet a bona fide medical emergency in which the patient's prior informed consent cannot be obtained.

1. Immediately following disclosure, the Privacy Official shall document, in writing, the disclosure in the patient's records, including:

i. The name of the medical personnel to whom disclosure was made and their affiliation with any health care facility;

ii. The name of the individual making the disclosure;

iii. The date and time of the disclosure; and

iv. The nature of the emergency.

G. To the Federal Food and Drug Administration. Chimes may disclose patient identifying information to medical personnel of the Food and Drug Administration (FDA) who assert a reason to believe that the health of any individual may be threatened by an error in the manufacture, labeling, or sale of a product under FDA jurisdiction, and that the information will be used for the exclusive purpose of notifying patients or their physicians of potential dangers.

1. Immediately following disclosure, the Privacy Official shall document, in writing, the disclosure in the patient's records, including:

i. The name of the medical personnel to whom disclosure was made and their affiliation with any health care facility;

ii. The name of the individual making the disclosure;

iii. The date and time of the disclosure; and

iv. The nature of the error.

H. Research. In limited situations, Chimes may disclose patient identifying information for the purpose of conducting scientific research. The Privacy Official, who may consult with legal counsel, shall be consulted prior to any disclosure for research purposes.

I. Audits and Evaluations. In limited circumstances, Chimes may disclose Substance Use Disorder Information without patient consent to federal, state, and local governments to allow these governmental entities to carry out audits and evaluations. Any such requests are directed to the Privacy Official, who may

consult with legal counsel, before any disclosure is made in connection with an audit or evaluation.

J. Subpoenas. In limited situations, Chimes may disclose Substance Use Disorder Information in response to a subpoena, if a court order that satisfies specific requirements to protect the Substance Use Disorder Information has been entered by the court. Subpoenas shall immediately be forwarded to the Privacy Official, who may consult with legal counsel, prior to any disclosure in response to a subpoena.

K. Court Orders. In limited situations, Chimes may disclose Substance Use Disorder Information pursuant to a court order satisfying specific conditions. Any such requests are directed to the Privacy Official, who may consult with legal counsel, before any disclosure is made in connection with an audit or evaluation.

III. **Minimum Necessary**. Chimes limits the disclosure of Substance Use Disorder to that which is necessary to carry out the purpose of the disclosure. Please see Chimes' "Minimum Necessary" policy (P010).

IV. Chimes limits its uses and disclosures of Substance Use Disorder as set forth above, even if the person seeking the information already has it, has other means of obtaining it, is a law enforcement agency or official or other government official, has obtained a subpoena, or asserts any other justification.

REGULATORY REFERENCES

42 CFR § 2.12
42 CFR § 2.13
42 CFR § 2.13(c)(2)
42 CFR § 2.15
42 CFR § 2.21
42 CFR § 2.53
42 CFR § 2.51
42 CFR § 2.52
42 CFR Part 2, Subpart E

Chimes Privacy Policies & Procedures	
Title: Uses and Disclosures of PHI - Overview	**No. P013**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2023	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes will only use and disclose PHI as permitted or required by HIPAA and applicable state law.

Substance Use Disorder Information shall only be disclosed in accordance with Chimes' "Use and Disclosure of Substance Use Disorder Information" policies (P012 and subparts).

PROCEDURES

I. General Procedures

A. Chimes will only use and disclose PHI as permitted or required by HIPAA and applicable state law.

1. *To the Individual*. Chimes will disclose PHI to the individual who is the subject of the information.

2. *Pursuant to a valid Authorization*. Chimes will disclose PHI pursuant to a valid HIPAA authorization. Please see Chimes' "Authorizations for Uses and Disclosures" policy (P007).

3. *Business Associates*

i. Chimes may disclose PHI to a business associate, if:

a. The PHI requested is necessary for the business associate to perform services as provided for by a services agreement; and

b. Chimes has executed a proper business associate agreement. Please see Chimes' "Business Associates and Qualified Service Organizations" policy (P023).

4. *When legally required*. Chimes shall disclose PHI when it is required to do so by federal, state, or local law. Disclosures shall be limited to the relevant requirements of such law. The Privacy Official shall be notified of any request to disclose PHI pursuant to federal, state, or local law. Legal counsel shall be consulted prior to disclosure.

B. Workforce members, after approval by the Privacy Official, may use and disclose PHI in accordance with the procedures set forth in the following:

1. P013.01 – Uses and Disclosures of PHI – Psychotherapy Notes

2. P013.02 – Uses and Disclosures of PHI – Treatment, Payment, Healthcare Operations

3. P013.03 – Uses and Disclosures of PHI – Law Enforcement

4. P013.04 – Uses and Disclosures of PHI – Abuse, Neglect, and Domestic Violence

5. P013.05 – Uses and Disclosures of PHI – Judicial and Administrative Proceedings

6. P013.06 - Uses and Disclosures of PHI – Public Health

7. P013.07 – Uses and Disclosures of PHI – Persons Involved in Care; Notification; Facility Directory

8. P013.08 – Uses and Disclosures of PHI – De-Identification of PHI and Limited Data Sets

9. P013.09 – Uses and Disclosures of PHI – Fundraising

10. P013.10 – Uses and Disclosures of PHI – Marketing

11. P013.11 – Uses and Disclosures of PHI – Research

C. Workforce members and the Privacy Official shall ensure that all uses and disclosures are consistent with Chimes' current Notice of Privacy Practices.

D. Workforce members shall consult with the Privacy Official prior to using or disclosing information regarding mental health, developmental disabilities, or communicable diseases. The Privacy Official will only approve any such use or disclosure as permitted by state and federal law. For example:

1. Under Maryland law, when a medical record developed in connection with the provision of mental health services is disclosed without the authorization of a person in interest, only the information in the record relevant to the purpose for which disclosure is sought may be released. (Md. Code Ann. Health—Gen. § 4-307).

2. Under Pennsylvania law, all documents concerning persons in treatment for mental illness shall be kept confidential and, without the person's written consent, may not be released or their contents disclosed to anyone except: (1) those engaged in providing treatment for the person; (2) the county administrator in certain instances; (3) a court in the course of legal proceedings authorized by this act; (4) pursuant to Federal rules, statutes and regulations governing disclosure of patient information where treatment

is undertaken in a Federal agency; and (5) a covered entity or a covered entity's business associate that makes the use, disclosure or request for disclosure in accordance with 45 C.F.R. Pt. 164 Subp. E (relating to privacy of individually identifiable health information). (50 Pa. Stat. Ann. § 7111).

3. New Jersey law requires records regarding mental health to be kept confidential and not disclosed, except when (1) there is proper consent, (2) the disclosure of necessary to comply with New Jersey law, a court directs the disclosure, (4) the disclosure is necessary to conduct an investigation into the financial ability to pay; or (5) the disclosure is needed to comply with the data reporting provisions of the NICS Improvement Amendments Act of 2007 and the Brady Handgun Violence Prevention Act of 1993. (N.J. Stat. Ann. § 30:4-24.3).

E. Workforce members shall ensure that any use or disclosure is not prohibited by a restriction in place pursuant to Chimes' "Requests for Restrictions and Confidential Communications" policy (P022).

F. Incidental Disclosures.

1. Chimes has implemented, and all workforce members are expected to comply with, this Program and the administrative, technical and physical safeguards implemented based upon Chimes' operations, including the minimum necessary requirements.

2. A permitted incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and occurs as a result of another use or disclosure that is permitted by HIPAA.

3. An incidental use or disclosure is not permitted if it is a by-product of an underlying use or disclosure which violates the Privacy Rule.

G. Except as otherwise provided, uses and disclosures of PHI shall comply with Chimes' "Minimum Necessary" policy (P010).

H. Substance Use Disorder Information shall only be disclosed in accordance with Chimes' "Use and Disclosure of Substance Use Disorder Information" policies (P012 and subparts).

I. The Privacy Official shall track disclosures in accordance with Chimes' "Tracking and Accounting of Disclosures" policy (P021). Records of disclosures should be kept for at least six (6) years after the disclosure is made.

II. Prohibition on Sale of PHI.

A. Chimes does not typically sell PHI. The sale of PHI includes any disclosure in exchange for, directly or indirectly, financial remuneration.

B. All sales of PHI must be approved by the Privacy Official, the Corporate Privacy Official, and legal counsel. The Privacy Official shall document the rationale for any approval. Approval shall only occur in the following instances:

1. The individual has signed a valid authorization, which includes a statement that Chimes will receive remuneration. Please see Chimes' "Authorizations for Uses and Disclosures" policy (P007).

2. The sale is permitted by HIPAA and applicable law, and no authorization is required.

III. Questions. Any questions about uses and disclosures should be directed to the Privacy Official. The Privacy Official, with legal counsel, if necessary, shall make determinations regarding non-routine uses, disclosures, or requests for PHI on a case-by-case basis.

REGULATORY REFERENCES

45 CFR § 164.502(i)
45 CFR § 164.508(a)(4)
45 CFR § 164.512(a)

Chimes Privacy Policies & Procedures	
Title: Uses and Disclosures of PHI - Psychotherapy Notes & SUD Counseling Notes	**No. P013.01**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes treats mental health records and psychotherapy notes and Substance Use Disorder (SUD) Counseling notes with the utmost confidentiality. Mental health records include any information obtained or records prepared in the course of providing any mental health services. Psychotherapy notes and SUD Counseling notes include those notes recorded (in any medium) by a health care provider, who is a mental health and or substance use disorder treatment professional, that document or analyze the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record.

Workforce members may only use and disclose psychotherapy notes and SUD Counseling notes in accordance with this Policy.

PROCEDURES

I. Workforce members shall consult with the Privacy Official prior to using or disclosing psychotherapy notes and SUD Counseling notes. The Privacy Official will only approve any such use or disclosure as permitted by state and federal law.

II. **Authorization Required.** In general, Chimes cannot disclose mental health and substance us disorder treatment records without the patient's authorization.

A. Prior to using or disclosing psychotherapy notes or SUD Counseling notes, the Privacy Official will ensure that Chimes has obtained the individual's authorization, consistent with Chimes' "Authorizations for Uses and Disclosures" policy (P007), *except for the instances set forth below.*

B. With the prior approval of the Privacy Official, an authorization may not be required if the use or disclosure is:

1. To carry out the following treatment, payment, or health care operations purposes:

i. Use by the originator of the psychotherapy notes or SUD Counseling notes for treatment;

ii. Use or disclosure by Chimes for its own training programs in which students, trainees, or practitioners in mental health and or Substance

Use Disorder treatment learn under supervision to practice or improve their skills in group, joint, family, or individual counseling;

iii. Use or disclosure to defend Chimes in a legal action or other proceeding brought by the patient;

iv. Disclosure necessary to assure service or care to the patient by the least drastic means that are suitable to the patient's liberty and interests; or

v. Disclosure necessary for continuity of care when a patient moves from one service provider to another.

2. A use or disclosure that is:

i. Required by the Office for Civil Rights of HHS to investigate or determine Chimes' compliance with HIPAA;

ii. Required by a law, complies with such law, and is limited to the relevant requirements of such law;

iii. Made to a health oversight agency authorized by law to conduct health oversight of the originator of the psychotherapy notes;

iv. Made to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by applicable state law;

v. Consistent with law and the standards of ethical conduct, if Chimes, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat;

vi. Solely information as to a residential patient's overall medical condition without clinical details and is sought by the patient's family members, relatives, conservator, legal guardian, legal custodian, guardian ad litem, foster parents, or friends;

vii. Made pursuant to a court order, upon the court's determination, after a hearing, that disclosure is necessary for the conduct of proceedings before it and that failure to make such disclosure would be contrary to public interest or to the detriment of a party to the proceeding; or

viii. Necessary because a custodial agent for another state agency that has legal custody of the patient cannot perform the agent's duties properly without the information.

III. Questions – Workforce members shall consult with the Privacy Official should there be any questions regarding uses, disclosures, and requests for PHI. The Privacy Official and legal counsel, if necessary, shall make determinations on a case-by-case basis.

REGULATORY REFERENCES

45 CFR § 164.508(e)(2)

42 CFR § 2.31

Chimes Privacy Policies & Procedures	
Title: Uses and Disclosures of PHI – Treatment, Payment & Health Care Operations	**No. P013.02**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes will only use and disclose protected health information (PHI) as permitted or required by HIPAA and applicable state law. Workforce members may use and disclose PHI for treatment, payment, and health care operations purposes as set forth in this Policy.

Substance Use Disorder Information shall only be disclosed in accordance with Chimes' "Use and Disclosure of Substance Use Disorder Information" policies (P012 and subparts). Psychotherapy notes, SUD Counseling notes and mental health records shall only be disclosed in accordance with Chimes' "Use and Disclosure of PHI – Psychotherapy Notes & SUD Counseling Notes" policy (P013.01).

PROCEDURES

I. Use and Disclosure of PHI for Treatment, Payment, and Health Care Operations Purposes.

A. Uses and Disclosures for Chimes' Purposes. Workforce members may use or disclose PHI for Chimes' own treatment, payment, and health care operations activities.

1. Uses and disclosures for payment and health care operations purposes are subject to Chimes' "Minimum Necessary" policy (P010). When members of workforce provide treatment, they are permitted to use PHI without being restricted by the minimum necessary policy. This would not include any activities performed by administrative staff.

i. Examples of payment and health care operations include, but are not limited to:

a. Uses and disclosures for billing, claims management, collection activities and obtaining payment;

b. Quality assessment, credentialing, accreditation or licensing activities;

c. Appeals of adverse benefit determinations;

d. Conducting or arranging for auditing, medical review or legal services; and

e. Health care operations within the meaning of HIPAA regulations, 45 CFR § 164.501.

2. When disclosing PHI to an individual or entity in order for the individual or entity to assist Chimes with payment and health care operations, the Privacy Official shall ensure that Chimes has entered into a business associate agreement with the third-party service provider.

B. Uses and Disclosures for Another's Purposes.

1. Workforce members may disclose PHI to another health care provider for the recipient's treatment activities.

2. Workforce members may disclose PHI to another covered entity or health care provider for the recipient's payment activities.

3. Workforce members may disclose PHI to another covered entity for the recipient's health care operations activities, if:

i. Both covered entities have or had a relationship with the individual who is the subject of the PHI;

ii. The PHI pertains to such relationship; and

iii. The disclosure is for the purpose of:

a. Health care fraud and abuse detection or compliance; or

b. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that research (*i.e.*, the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities); patient safety activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination; contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; or

c. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, 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, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities.

C. Workforce members may not use or disclose psychotherapy notes, engage in marketing, or engage in the sale of PHI under this policy.

D. Workforce members may obtain consent to use or disclose PHI to carry out treatment, payment, or health care operations. However, consent shall not be effective when an authorization is required or when another condition must be met with respect to the contemplated use or disclosure.

II. Questions. – Workforce members shall consult with the Privacy Official should there be any questions regarding uses, disclosures, and requests for PHI. The Privacy Official and legal counsel, if necessary, shall make determinations on a case-by-case basis.

REGULATORY REFERENCES

45 CFR § 164.506(a)
45 CFR § 164.506(b)

Chimes Privacy Policies & Procedures	
Title: Uses and Disclosures of PHI – Law Enforcement	**No. P013.03**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2023	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes will only use and disclose protected health information (PHI) as permitted or required by HIPAA and applicable state law. Workforce members may use and disclose PHI for law enforcement purposes, to correctional facilities, and for specialized government functions as set forth in this Policy.

Substance Use Disorder Information shall only be disclosed in accordance with Chimes' "Use and Disclosure of Substance Use Disorder Information" policies (P012 and subparts). Psychotherapy notes, SUD Counseling notes and mental health records shall only be disclosed in accordance with Chimes' "Use and Disclosure of PHI – Psychotherapy Note & SUD Counseling notes" policy (P013.01).

PROCEDURES

I. General Procedures.

A. With the prior approval of the Privacy Official, workforce members may disclose PHI to law enforcement officials for the purposes outlined below.

B. The identity and authority of individuals requesting PHI must be verified. Please see Chimes' "Verification" policy (P009).

C. Workforce members shall immediately contact the Privacy Official, who may contact the legal counsel, upon:

1. Receipt of an inquiry or notice of investigation by mail;

2. Receipt of a request for information for law enforcement purposes from a law enforcement officer, including any of the following:

i. A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;

ii. A grand jury subpoena;

iii. An administrative request, including an administrative subpoena or summons, or a civil or an authorized investigative demand, or similar process authorized under law; or

iv. A request for information about a patient who is or is suspected to be a victim of a crime.

3. An on-site search or request.

D. Workforce members shall consult with the Privacy Official prior to making any disclosures addressed in this Policy. The Privacy Official shall approve all such disclosures and may only do so in accordance with this Policy and as permitted or required by law.

II. Law Enforcement

A. Required by Law. With the prior approval of the Privacy Official, workforce members may disclose PHI as required by law, including:

1. Those laws that require the reporting of certain types of wounds or injuries, as approved by the Privacy Official.

2. If the information sought is relevant and material to a legitimate law enforcement inquiry and de-identified information cannot be used, in response to specific and limited requests in the following:

i. A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;

ii. A grand jury subpoena;

iii. An administrative request, including an administrative subpoena or summons, or a civil or an authorized investigative demand, or similar process authorized under law; or

iv. A request for information about a patient who is or is suspected to be a victim of a crime.

B. Identification or Location Purposes. With the prior approval of the Privacy Official, workforce members may disclose PHI for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person. For this purpose, workforce members may not disclose PHI related to the individual's DNA or DNA analysis, dental record, or typing, samples or analysis of body fluids or tissue. Workforce members may disclose only the following PHI for this purpose:

1. Name and address;

2. Date and place of birth;

3. Social Security number;

4. ABO blood type and Rh factor;

5. Type of injury;

6. Date and time of treatment;

7. Date and time of death, if applicable; and

8. A description of distinguishing physical characteristics.

C. Information about Crime Victims. With the prior approval of the Privacy Official, workforce members may disclose PHI in response to a law enforcement official's request for PHI about an individual who is, or is suspected to be, a victim of a crime, provided that:

1. The individual agrees to the disclosure; or

2. If the individual is unable to agree because of incapacity or other emergency circumstances, the law enforcement official represents that the PHI is needed to determine whether a violation of the law has occurred, the PHI is not intended to be used against the victim, the immediate law enforcement activity depends upon the disclosure and would be materially and adversely affected by waiting until the patient can agree, and Chimes determines that disclosure is in the patient's best interests.

D. Information about Decedents**.** With the prior approval of the Privacy Official, workforce members may disclose PHI about an individual who has died to alert law enforcement of the death if the workforce member has a reasonable suspicion that such death resulted from criminal conduct.

E. Crime on Premises. With the prior approval of the Privacy Official, workforce members may disclose PHI about an individual if the workforce member believes in good faith that PHI constitutes evidence of criminal conduct that occurred on the premises of Chimes.

F. Disclosures by Workforce Members Who are Victims of Crimes. Chimes will not be in violation of HIPAA if a member of its workforce who is the victim of a crime discloses any of the following PHI (but no other PHI) about the suspected perpetrator to a law enforcement official:

1. Name and address;

2. Date and place of birth;

3. Social security number;

4. ABO blood type and rh factor;

5. Type of injury;

6. Date and time of treatment;

7. Date and time of death, if applicable; and

8. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

G. Other. Workforce members may disclose PHI about an individual while providing emergency care in response to a medical emergency, to alert law enforcement to the commission and nature of a crime; the location of such crime; the victims of such crime; and the identity, description, and locations of the perpetrator of such crime. This section does not apply if the emergency is the reuse of abuse, neglect, or domestic violence.

III. Correctional Institutions

A. With the prior approval of the Privacy Official, workforce members may disclose PHI about an inmate or other individual to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual if the correctional institution or such law enforcement official represents says that such health information is necessary for:

1. The provision of health care to such individuals;

2. The health and safety of such individual or other inmates;

3. The health and safety of the officers or employees of or others at the correctional institution;

4. The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility or setting to another;

5. Law enforcement on the premises of the correctional institution; or

6. The administration and maintenance of the safety, security and good order of the correctional institution.

B. An individual is no longer an inmate when released on parole, probation, supervised release, or otherwise no longer in lawful custody.

IV. Specialized Government Functions

A. Military and Veterans Activities

1. With the prior approval of the Privacy Official, workforce members may use and disclose the PHI of the patients who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the Federal Register the following information:

i. Appropriate military command authorities; and

ii. The purposes for which the PHI may be used or disclosed.

B. National Security and Intelligence Activities. With the prior approval of the Privacy Official, workforce members may disclose PHI to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act, codified at 50 USC § 401, *et seq*., and implementing authority (for example, Executive Order 12333).

C. Protective Services for the President and Others. With the prior approval of the Privacy Official, workforce members may disclose PHI to authorized federal officials for the provisions of protective services to the President or other persons as authorized by 18 USC § 3056, or to foreign heads of state or other persons authorized by 22 USC § 2709(a)(3), or for the conduct of investigations authorized by 18 USC §§ 871 and 879.

D. Requests from Foreign Military Authorities. All requests for PHI from foreign military authorities will be sent to the Privacy Official immediately. Chimes may disclose PHI of individual who are foreign military personnel to their appropriate foreign military personnel to assure the proper execution of the military mission.

V. Questions. Workforce members shall consult with the Privacy Official should there be any questions regarding uses, disclosures, and requests for PHI. The Privacy Official and legal counsel, if necessary, shall make determinations on a case-by-case basis.

REGULATORY REFERENCES

45 CFR § 164.502(j)(2)
45 CFR § 164.512(a)
45 CFR § 164.512(f)(1)
45 CFR § 164.512(f)(2)
45 CFR § 164.512(f)(3)
45 CFR § 164.512(f)(4)
45 CFR § 164.512(f)(5)
45 CFR § 164.512(f)(6)
45 CFR § 164.512(k)(1)
45 CFR § 164.512(k)(2)
45 CFR § 164.512(k)(3)
45 CFR § 164.512(k)(5)

Chimes Privacy Policies & Procedures	
Title: Uses and Disclosures of PHI – Abuse, Neglect, and Domestic Violence	**No. P013.04**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1-16-26

POLICY

Chimes Behavioral Health Systems ("Chimes") will only use and disclose protected health information (PHI) as permitted or required by HIPAA and applicable state law. Workforce members may use and disclose PHI in reporting abuse, neglect, and domestic violence as set forth in this Policy.

Substance Use Disorder Information shall only be disclosed in accordance with Chimes' "Use and Disclosure of Substance Use Disorder Information" policies (P012 and subparts). Psychotherapy notes, SUD Counseling notes and mental health records shall only be disclosed in accordance with Chimes' "Use and Disclosure of PHI – Psychotherapy Note & SUD Counseling notes" policy (P013.01).

PROCEDURES

I. Child Abuse or Neglect. Workforce members are mandated reporters. Therefore, workforce members, with the approval of the Privacy Official, may disclose PHI without the patient's authorization to a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect.

A. Under Delaware law, any report of child abuse or neglect must be made by contacting the Child Abuse and Neglect Report Line for the Department of Services for Children, Youth and Their Families. An immediate oral report must be made by telephone or otherwise. (16 Del. C. §§ 903 and 904).

B. Under Maryland law, the required oral/telephone reports should be given to the local child protective services office as soon as is possible, and a written report should be provided within 48 hours. The written report is also required to be given to the state's attorney. (Md. Code Ann., Fam. Law § 5-704).

C. Under New Jersey law, any person having reasonable cause to believe that a child has been subjected to child abuse or acts of child abuse shall report the same immediately to the Division of Child Protection and Permanency by telephone or otherwise. (N.J. Stat. Ann. § 9:6-8.10).

D. Under Pennsylvania law, an oral report of suspected child abuse must be made immediately to the department via the statewide toll-free telephone number ((800) 932-0313) or the online portal and submit a written report within 48 hours to the agency assigned to assist with the matter. (23 Pa. Stat. and Cons. Stat. Ann. § 6313).

E. Under Virginia law, a mandated reporter, which includes all those within the healing arts, must report, which may be oral, suspected abuse or neglect of a child, immediately to the local department of the county of city wherein the child resides or wherein the abuse or neglect is believed to have occurred. (Va. Code Ann. §63.2-1509).

II. Abuse, Neglect, or Domestic Violence.

A. In cases that do not involve reports of child abuse or neglect (see above), workforce members may, with approval from the Privacy Official, disclose PHI about an individual whom Chimes reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence if:

1. The patient agrees to the disclosure;

2. The disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law; or

3. Chimes is expressly permitted by law to make the disclosure and:

i. Chimes, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the patient or other potential victims; or

ii. The patient is unable to agree to the disclosure because of incapacity, and a law enforcement or other public official authorized to receive the report represents that:

a. The PHI for which disclosure is sought is not intended to be used against the patient; and

b. An immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the patient is able to agree to the disclosure.

iii. Such disclosures may only be made to a government authority authorized by law to receive reports of abuse, neglect or domestic violence.

B. The treating physician shall inform the patient that a report has been (or will be) made, unless:

1. Chimes, in the exercise of professional judgment, believes informing the patient would place the patient at risk of serious harm; or

2. Chimes would be informing a personal representative, and Chimes reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing such person would not be in the best interests of the patient as determined by Chimes, in the exercise of professional judgment.

III. Questions. Workforce members shall consult with the Privacy Official should there be any questions regarding uses, disclosures, and requests for PHI.

REGULATORY REFERENCES

45 CFR § 164.512(a)
45 CFR § 164.512(b)
45 CFR § 164.512(c)

Chimes Privacy Policies & Procedures	
Title: Uses and Disclosures of PHI – Judicial and Administrative Proceedings	**No. P013.05**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes will only use and disclose protected health information (PHI) as permitted or required by HIPAA and applicable state law. Workforce members may use and disclose PHI in judicial and administrative proceedings as set forth in this Policy.

Substance Use Disorder Information shall only be disclosed in accordance with Chimes' "Use and Disclosure of Substance Use Disorder Information" policies (P012 and subparts). Psychotherapy notes, SUD Counseling notes and mental health records shall only be disclosed in accordance with Chimes' "Use and Disclosure of PHI – Psychotherapy Note & SUD Counseling notes" policy (P013.01).

PROCEDURES

I. General Procedures

A. Workforce members shall immediately forward any and all requests for PHI in connection with any judicial or administrative proceeding to the Privacy Official, who shall consult with legal counsel.

B. Subject to the requirements of Section I.A., above, Chimes may disclose PHI when requested by subpoena or other legal document or without the patient's authorization when permitted to do so under HIPAA.

II. Judicial and administrative proceedings

A. If the request specifies Chimes or requests information maintained by Chimes, the workforce members shall consult with legal counsel and/or the Privacy Official.

B. Chimes may disclose PHI in the course of a judicial or administrative proceeding in response to an order of a court or administrative tribunal. The Privacy Official shall ensure that Chimes only discloses the PHI expressly authorized by the order.

C. Chimes may disclose PHI in response to a subpoena, discovery request, or other lawful process that is not accompanied by an order, if Chimes receives:

1. Satisfactory assurances from the party seeking the PHI that the party has made reasonable efforts to ensure that the individual to whom the requested PHI pertains has been given notice of the request. Chimes has such assurance if the party seeking the PHI has demonstrated with supporting documentation:

i. That such party made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);

ii. The notice included enough information about the litigation or proceeding to allow the individual to raise an objection with the court or administrative tribunal; and

iii. The time for the individual to raise objections with the court or administrative tribunal has lapsed (generally 14 days from the day the notice was served on the individual) and no objection was filed or any objection filed has been resolved and disclosure of the PHI is consistent with that resolution.

2. Satisfactory assurances from the party seeking the PHI that reasonable efforts have been made by the party seeking the PHI to secure a "qualified protective order." A "qualified protective order" is an order from a court or administrative tribunal or a joint stipulation by the parties that prohibits the parties from using or disclosing the PHI for any purpose other than the proceeding and requires the PHI and all copies to be returned to Chimes at the end of the proceeding. Chimes has such assurance if the party seeking the PHI has demonstrated with supporting documentation that:

i. The parties to the dispute giving rise to the request for PHI have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

ii. The party seeking the PHI has requested a qualified protective order from such court or tribunal.

D. If the court order, administrative tribunal order, subpoena, discovery request or other lawful process seeks to require a workforce member to testify before the court, administrative tribunal or in a deposition, the workforce member must inform his or her supervisor and the Privacy Official immediately upon receiving the subpoena or other request. The Privacy Official shall consult legal counsel immediately, as appropriate. Legal counsel will determine whether and how the workforce member will comply with the subpoena or other request.

III. Questions. Workforce members shall consult with the Privacy Official should there be any questions regarding uses, disclosures, and requests for PHI.

REGULATORY REFERENCES

45 CFR § 164.512(a)
45 CFR § 164.512(e)

Chimes Privacy Policies & Procedures	
Title: Uses and Disclosures of PHI – Public Health	**No. P013.06**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes will only use and disclose protected health information (PHI) as permitted or required by HIPAA and applicable state law. Workforce members may use and disclose PHI for public health purposes as set forth in this Policy.

Substance Use Disorder Information shall only be disclosed in accordance with Chimes' "Use and Disclosure of Substance Use Disorder Information" policies (P012 and subparts). Psychotherapy notes, SUD Counseling notes and mental health records shall only be disclosed in accordance with Chimes' "Use and Disclosure of PHI – Psychotherapy Note & SUD Counseling notes" policy (P013.01).

PROCEDURES

I. Public Health Activities. Workforce members shall consult with the Privacy Official prior to using or disclosing any PHI in connection with public health activities.

A. Public Health Reporting

1. With the prior approval of the Privacy Official, workforce members may disclose PHI without the patient's authorization to a public health authority that is authorized by law to collect or receive such information for the purposes of:

   i. Preventing or controlling disease, injury, or disability, including but not limited to the reporting of disease, injury, vital events such as birth or death. For example:

      a. Under Delaware law, a health care provider who diagnoses a child with autism must report occurrences of autism in any child in the state. (Del. Code Ann. tit. 16, § 223).

      b. Under Pennsylvania law, an event, occurrence or situation involving the clinical care of a patient in a medical facility that (1) results in death or compromises patient safety and results in an unanticipated injury requiring the delivery of additional health care services to the patient; and (2) which could have injured the patient but did not either cause an unanticipated injury or require the delivery of additional health care services to the patient must be reported to the Department of Health and the Patient Safety Authority

within 24 hours of the medical facility's confirmation of the occurrence of the serious event. (40 Pa. Stat. Ann. §§ 1303.308 and 1303.313).

ii. The conduct of public health surveillance, public health investigations, and public health interventions; or

iii. At the direction of a public health authority, to an officer of a foreign government agency that is acting in collaboration with a public health authority.

B. FDA Reporting

1. With the prior approval of the Privacy Official, workforce members may disclose PHI to a person subject to the jurisdiction of the FDA with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:

i. To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;

ii. To track FDA-regulated products;

iii. To enable product recalls, repairs or replacement, or look-back (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of look-back); or

iv. To conduct post-marketing surveillance.

C. Communicable Diseases

1. With the prior approval of the Privacy Official, workforce members may disclose PHI without the patient's authorization to alert a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition if Chimes is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation.

D. Disclosures to Employers. With the prior approval of the Privacy Official, workforce members may report information to an individual's employer if:

1. Chimes provides a health care service to the patient at the request of the employer either to (i) conduct an evaluation relating to medical surveillance

of the workplace or (ii) evaluate whether the patient has a work-related illness or injury;

2. The PHI that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;

3. The employer needs such findings in order to comply with its obligations under OSHA or the Mine Safety and Health Act, or under any state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and

4. Chimes provides written notice to the patient that the PHI relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:

   i. By giving a copy of the notice to the patient at the time the health care is provided; or

   ii. If the health care is provided on the worksite of the employer, by posting the notice in a prominent place at the location where the health care is provided.

E. Disclosures to a School. With the prior approval of the Privacy Official, workforce members may disclose PHI to a school, about an individual who is a student or prospective student of the school, if:

1. Chimes obtains and documents the agreement to the disclosure from either:

   i. A parent, guardian, or other person acting *in loco parentis* of the individual, if the individual is an un-emancipated minor; or

   ii. The individual, if the individual is an adult or an emancipated minor.

II. Health Oversight Activities

A. If Chimes receives a request for disclosure from a health oversight agency in connection with an activity such as an audit, investigation, inspection, licensure or disciplinary action, civil, administrative, or criminal proceeding or action, the receiving workforce member shall immediately contact the Privacy Official to determine how to respond.

B. Chimes may disclose PHI to a health oversight agency (U.S. Department of Health and Human Services or other agencies authorized by law) for oversight activities authorized by law, including audits; civil, administrative or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative or criminal proceedings or actions; or other activities necessary for appropriate oversight of:

1. The health care system;

2. Government benefit programs for which PHI is relevant to beneficiary eligibility;

3. Entities subject to government regulatory programs for which PHI is necessary for determining compliance with program standards; or

4. Entities subject to civil rights laws for which PHI is necessary for determining compliance.

C. For purposes of this section, a health oversight activity does not include an investigation or other activity in which the patient is the subject of the investigation or activity and such investigation/activity is not related to the receipt of health care, a claim for public benefits related to health, or qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services. However, if a health oversight investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity

D. Chimes is required to disclose PHI to the Secretary of the U.S. Department of Health & Human Services or, the Secretary's designee, when the Secretary is investigating or auditing Chimes to determine Chimes' compliance with HIPAA and other applicable state and federal laws and regulations. Legal counsel should be consulted to verify authenticity.

III. Decedents

A. Coroners & Medical Examiners. Chimes may disclose PHI to coroners and medical examiners for the following purposes:

1. To identify a deceased person;

2. To determine a cause of death; or

3. As otherwise authorized by law.

B. Funeral Directors. Chimes may disclose PHI to funeral directors, consistent with applicable law, as needed for funeral directors to carry out their duties with respect to the decedent. If necessary, Chimes may disclose PHI prior to, and in reasonable anticipation of, the patient's death.

IV. Organ and Tissue Procurement

Organ and Tissue Procurement. Workforce members may disclose PHI to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for donation or transplantation.

V. To Avert a Serious Threat to Health or Safety

To Avert a Serious Threat to Health or Safety.

A. Workforce members shall consult the Privacy Official to determine whether

HIPAA and other applicable laws permit disclosure of PHI for purposes of averting a serious threat to health or safety.

1. The workforce member must believe in good faith that such disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, and the use or disclosure must be to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or

2. The use or disclosure is necessary for law enforcement authorities to identify or apprehend an patient where it appears from all the circumstances that the patient has escaped from a correctional institution or from lawful custody; or

3. The use or disclosure is necessary for law enforcement authorities to identify or apprehend a patient because of a statement by a patient admitting participation in a violent crime that we reasonably believe may have caused serious physical harm to the victim.

VI. Disaster Relief Agencies

A. Chimes may use or disclose PHI to an authorized public or private disaster relief agency for the purpose of helping such entity notify an individual's family member, personal representative, or another person responsible for the individual's care, of the individual's location, general condition, or death. Workforce members will comply with the procedures discussed below if in their professional judgment they determine that doing so will not interfere with the ability to respond to the emergency circumstances:

1. If the patient is present or otherwise available, prior to a disclosure of PHI to a disaster relief organization, the workforce member shall:

   i. Obtain the patient's agreement;

   ii. Provide the patient with the opportunity to object to the disclosure, and the patient has not expressed an objection; or

   iii. Reasonably infer from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.

2. If the patient is not present or otherwise available because the patient is incapacitated or under an emergency circumstance, a workforce member shall only disclose PHI to a disaster relief organization, if:

   i. The workforce member (a) has determined, in the exercise of professional judgment, that the disclosure is in the best interests of

the individual; and (b) discloses only the PHI that is directly relevant to the individual's care.

ii. Chimes will not disclose PHI to friends or family members in cases of abuse, neglect, or domestic violence.

B. If the requirements listed above would interfere with the ability of the disaster relief organization to respond to an emergency, workforce members, in the exercise of professional judgment, may disclose PHI without obtaining the individual's consent.

VII. Workers' Compensation

A. Workforce members may disclose PHI as authorized and to the extent necessary to comply with laws regarding workers' compensation and other similar programs that are established under law and provide benefits for work-related injuries/illness without regard to fault.

REGULATORY REFERENCES

45 CFR § 164.510(b)(4)
45 CFR § 164.512(a)
45 CFR § 164.512(b)
45 CFR § 164.512(d)
45 CFR § 164.512(g)
45 CFR § 164.512(h)
45 CFR § 164.512(k)(1)
45 CFR § 164.512(k)(2)
45 CFR § 164.512(k)(3)
45 CFR § 164.512(k)(5)
45 CFR § 164.512(l)

Chimes Privacy Policies & Procedures	
Title: Uses and Disclosures of PHI – Persons Involved in Care; Notification; Facility Directory	**No. P013.07**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes will only use and disclose protected health information (PHI) as permitted or required by HIPAA and applicable state law. In accordance with this Policy, workforce members may (a) disclose protected health information (PHI) to certain persons involved in an individual's care; (b) use or disclose PHI in order to notify certain persons of the individual's location, condition, or death; and (c) use and disclose PHI to maintain a facility directory.

Substance Use Disorder Information shall only be disclosed in accordance with Chimes' "Use and Disclosure of Substance Use Disorder Information" policies (P012 and subparts). Psychotherapy notes, SUD Counseling notes and mental health records shall only be disclosed in accordance with Chimes' "Use and Disclosure of PHI – Psychotherapy Note & SUD Counseling notes" policy (P013.01).

PROCEDURES

I. General Procedures

A. Workforce members may only use or disclose PHI as permitted or required by HIPAA and applicable state law.

B. Workforce members shall direct all questions to the Privacy Official.

II. Facility Directory.

A. Chimes does not maintain a public facility directory, as it does not provide inpatient care.

B. If Chimes determines it is appropriate to maintain a facility directory in the future, the Privacy Official and legal counsel shall implement appropriate procedures.

III. Individuals Involved in Care

A. Workforce members may typically disclose to a family member, other relative, or close personal friend of the individual, or any other person identified by the individual, PHI which is directly relevant to such person's involvement with the individual's health care or payment related to the patient's care.

B. Workforce members may typically use or disclose PHI when necessary to notify or assist in the notification of (including identifying and locating), a family member,

a personal representative, or another person responsible for the care of the individual of the individual's location, general condition, or death.

C. Uses and Disclosures in the Presence of the Individual. If an individual is present for, or available prior to, a use or disclosure to family members, friends or personal representatives, and has the capacity to make health care decisions, workforce members shall only make the use or disclosure if:

1. The workforce member obtains the individual's agreement;

2. The workforce member provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or

3. The workforce member reasonably infers from the circumstances based on the exercise of professional judgment that the individual does not object to the disclosure.

D. Uses and Disclosures When the Individual Is Incapacitated or Not Present. If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be given because of the individual's incapacity or an emergency circumstance, workforce members shall only make the use or disclosure if:

1. The workforce member (a) has determined, in the exercise of professional judgment, that the disclosure is in the best interests of the individual; and (b) discloses only the minimum necessary PHI that is directly relevant to the individual's care.

2. Chimes will not disclose PHI to friends or family members in cases of abuse, neglect, or domestic violence.

E. Disclosures When the Individual is Deceased. If the individual is deceased, Chimes may disclose to a personal representative, special administrator, executor of the decedent's estate, that PHI which is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to Chimes.

F. Disclosures to Parents, Guardians, and Others Acting *In Loco Parentis*

1. To the extent permitted or required by applicable state law, Chimes may disclose, or provide access to, PHI about an un-emancipated minor to a parent, guardian, or other person acting *in loco parentis*;

2. To the extent prohibited by applicable state law, Chimes may not disclose, or provide access to, PHI about an un-emancipated minor to a parent, guardian, or other person acting *in loco parentis*; and

3. Where the parent, guardian, or other person acting *in loco parentis*, is not the personal representative (guardian of person, health care agent or surrogate) and where there is no applicable access provision under State or other law, Chimes may provide or deny access to a parent, guardian, or other person acting *in loco parentis*, if such action is consistent with applicable law, provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.

REGULATORY REFERENCES

45 CFR § 164.502(f)
45 CFR § 164.510(a)(1)
45 CFR § 164.510(a)(2)
45 CFR § 164.510(a)(3)
45 CFR § 164.510(b)(1)
45 CFR § 164.510(b)(2)
45 CFR § 164.510(b)(3)
45 CFR § 164.510(b)(5)

Chimes Privacy Policies & Procedures	
Title: Uses and Disclosures of PHI - De-Identification of PHI and Limited Data Sets	**No. P013.08**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes may use or disclose de-identified information or a limited data set without obtaining an individual's authorization.

Chimes may use protected health information (PHI) to create de-identified information **if allowed** by HIPAA and, *if Chimes is acting as a business associate*, the terms of any controlling services agreement and business associate agreement. Any PHI that has been properly de-identified under HIPAA is no longer PHI and is not subject to HIPAA, unless it is re-identified or the code for re-identification is disclosed.

Chimes may disclose PHI in a limited data set if it enters into a data use agreement with the recipient of the limited data set and complies with the other requirements of the HIPAA Privacy Rule governing the use and disclosure of PHI in limited data sets.

Substance Use Disorder Information shall only be disclosed in accordance with Chimes' "Use and Disclosure of Substance Use Disorder Information" policies (P012 and subparts). Psychotherapy notes, SUD Counseling notes and mental health records shall only be disclosed in accordance with Chimes' "Use and Disclosure of PHI – Psychotherapy Note & SUD Counseling notes" policy (P013.01).

PROCEDURES

I. De-Identification

A. Creation. The Privacy Official will oversee and approve all activities involving the de-identification of PHI at Chimes.

1. With respect to PHI created, received, and/or maintained in its capacity as a covered entity, Chimes may use such PHI to create de-identified information if allowed by HIPAA.

2. With respect to PHI created, received, or maintained when acting as a business associate, Chimes may only use such PHI to create de-identified information if allowed by HIPAA and the controlling services agreement and business associate agreement.

3. Method of De-Identifying PHI. HIPAA provides two acceptable methods of de-identifying PHI such that it is no longer considered PHI. Workforce

members shall adhere to all requirements of one of these two methods when creating de-identified information.

i. **Method One - Removal of Identifiers**. All of the following identifiers pertaining to an individual and relatives, employers or household members of the individual must be removed, and Chimes must not have actual knowledge that the information could be used alone or in combination with other information to identify the individual. Workforce members shall take care to ensure that any free text or other unstructured data fields do not contain stray identifiers or information that could be used to re-identify the patient.

   a. Names;

   b. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, (except for the initial three digits of a zip code if the geographic unit formed by such three digits contains more than 20,000 people). If such geographic units contain 20,000 people or less, then the initial three digits of the zip codes must be changed to 000 and thus treat them as a single geographic area;

   c. All elements of dates (except year) related to an individual, including birth date, admission date, discharge date, date of death, and ages over 89 or any element of a date that is indicative of age over 89;

      1. *Exception*: Ages and date elements related to individuals over 89 may be aggregated into a single category of age 90 or older.

   d. Telephone numbers;

   e. Fax numbers;

   f. Email addresses;

   g. Social security numbers;

   h. Medical record numbers;

   i. Health plan beneficiary numbers;

   j. Account numbers;

   k. Certificate or license numbers;

l. Vehicle identifiers and serial numbers, including license plate numbers;

m. Device identifiers and serial numbers;

n. Web universal resource locators (URLs);

o. Internet protocol (IP) address numbers;

p. Biometric identifiers, including finger and voice prints;

q. Full face photographs or comparable images; and

r. Any other unique identifying number, characteristic, or code (excluding a code assigned solely for re-identification purposes that meets HIPAA requirements, as described below).

ii. **Method Two - Statistician Determination**. A person with appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods for rendering information not individually identifiable, determines that the risk that the information could be used, alone or in combination with other reasonably available information, to identify an individual is very small, and such determination, and the methods for making the determination, are documented.

a. The Privacy Official shall ensure that the expert has relevant professional experience and academic or other training, as well as actual experience using health information de-identification methodologies.

b. The Privacy Official shall request that the expert assess the expected change of computational capability and access to various data sources to determine an appropriate timeframe within which the information will be considered reasonably protected from identification. At the end of such timeframe, the Privacy Official shall examine whether future releases of the data should be subject to additional or different de-identification processes to maintain the very low risk of identification.

B. Use and Disclosure

1. PHI that has been de-identified in accordance with HIPAA is not considered PHI and may be used and disclosed without complying with HIPAA requirements.

2. Chimes will only determine that PHI is no longer individually identifiable if one of the above procedures has occurred.

C. Re-Identification. Chimes may assign a code or other means of record identification to allow information that is de-identified under the above procedures to be re-identified provided that:

1. The code or other means of record identification is not related to or derived from information about the individual and is not otherwise capable of being translated so as to identify the individual; and

2. Chimes does not use or disclose the code for any other purpose or disclose the mechanism for re-identification.

D. De-identified information that has been re-identified may not be disclosed or used except as otherwise permitted under Chimes' policies for disclosure and use of PHI.

II. Limited Data Sets

A. Chimes may, without the individual's authorization, use and disclose a limited data set for research, public health, or health care operations purposes if a data use agreement is obtained.

1. The Privacy Official will oversee and approve all activities involving limited data sets. Legal counsel must be consulted prior to releasing a limited data set.

2. If Chimes is acting as a business associate, the Privacy Official will ensure that the use or disclosure is permissible under the terms of the controlling service agreement and business associate agreement.

3. Chimes must limit the PHI included in a limited data set to the minimum necessary information needed for the research, public health, or health care operations purpose(s) specified in the Data Use Agreement.

B. In creating a limited data set, the Privacy Official will exclude the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

1. Names;

2. Postal address information, other than town, city, state or zip code;

3. Telephone numbers;

4. Fax numbers;

5. Electronic mail addresses;

6. Social Security numbers;

7. Medical record numbers;

8. Health plan beneficiary numbers;

9. Account numbers;

10. Certificate / license numbers;

11. Vehicle identifiers and serial numbers, including license plate numbers;

12. Device identifiers and serial numbers;

13. Web Universal Resource Locaters (URLs);

14. Internet protocol (IP) address numbers;

15. Biometric identifiers, including fingerprints and voice prints; and

16. Full-face photographic images and any comparable images.

C. If Chimes intends to disclose a limited data set, a data use agreement or a business associate agreement, depending on the circumstances, must be entered into with the party receiving the limited data set.

1. A data use agreement shall contain at least the following terms:

i. A provision outlining the purposes for which the recipient can use or disclose the limited data set. These purposes must be for research, public health, or health care operations;

ii. A statement that the recipient may not use or disclose the limited data set in a manner that would violate the HIPAA Privacy Rule if done by Chimes;

iii. A list of the names of all individuals or entities permitted to receive the limited data set under the data use agreement;

iv. A statement that the recipient agrees not to use or further disclose the patient information in the limited data set other than as agreed to in the data use agreement or as required by law;

v. A statement that the recipient agrees to use appropriate safeguards to prevent the use or disclosure of the patient information in the limited data set in any manner other than as agreed to in the data use agreement;

vi. A statement that the recipient agrees to report to Chimes any use or disclosure of the patient information the recipient becomes aware of that is not provided for by the data use agreement;

vii. A statement that the recipient agrees to ensure any agents to whom it provides the limited data set will follow the same restrictions and conditions with respect to the use, disclosure and protection of the data use set that apply to the recipient;

viii. A statement that the recipient will not identify the information in the limited data set or attempt to contact the individuals; and

ix. A provision permitting Chimes to terminate the data use agreement and use of the limited data set by the recipient if Chimes becomes aware of any pattern of behavior or activity or practice of the recipient which materially breaches or violates the data use agreement. The statement should further indicate that Chimes may report any such breach or violation to the Secretary of the Department of Health and Human Services.

2. The Privacy Official shall approve and oversee the execution of all data use agreements for the use or disclosure of a limited data set.

REGULATORY REFERENCES

45 CFR § 164.514(b)
45 CFR § 164.514(c)
45 CFR § 164.514(e)

Chimes Privacy Policies & Procedures	
Title: Uses and Disclosures of PHI - Fundraising	**No. P013.09**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes may only use or disclose protected health information (PHI) for fundraising purposes in accordance with the procedures set forth below.

Substance Use Disorder Information shall only be disclosed in accordance with Chimes' "Use and Disclosure of Substance Use Disorder Information" policies (P012 and subparts). Psychotherapy notes, SUD Counseling notes and mental health records shall only be disclosed in accordance with Chimes' "Use and Disclosure of PHI – Psychotherapy Note & SUD Counseling notes" policy (P013.01).

PROCEDURES

I. Permitted Uses and Disclosures Without an Authorization

A. Chimes may, without an authorization, only use or disclose to its institutionally-related not-for-profit charitable foundation (Chimes Foundation) the following PHI for purposes of raising funds for its own benefit:

1. Demographic information relating to a patient, including, without limitation, the patient's name, address, other contact information, age, gender, and date of birth;

2. Dates of health care services provided to the patient;

3. The department that treated the patient;

4. Treating physician;

5. Outcome information; and,

6. Health insurance status.

B. Workforce member shall consult with the Privacy Official, who shall consult the Corporate Privacy Official and legal counsel, prior to any use or disclosure of PHI for fundraising purposes.

II. **Notice**. The Privacy Official shall ensure that Chimes includes in its "Notice of Privacy Practices," a statement that Chimes may use or disclose the information listed above for fundraising purposes without first obtaining the individual's authorization and that the individual has a right to opt out of receiving fundraising communications from Chimes.

III. Opt-Out and No Conditioning.

A. With each fundraising communication made to an individual, the Privacy Official shall ensure that Chimes provides the individual a clear and conspicuous opportunity to elect to not receive any further fundraising communications. The opt-out mechanism shall be free and easy to use.

B. The Privacy Official shall ensure that Chimes does not make fundraising communications to an individual who has elected not to receive such communications.

C. Chimes does not condition treatment or payment with respect to an individual on the individual's choice regarding the receipt of fundraising communications.

D. Chimes may provide an individual who has elected not to receive further fundraising communications with a method to opt in to receiving such communications should the individual wish to do so in the future.

REGULATORY REFERENCES

45 CFR § 164.514(f)

Chimes Privacy Policies & Procedures	
Title: Uses and Disclosures of PHI - Marketing	**No. P013.10**
Responsible Party: Privacy Official	Implementation Date: December 1, 2018
Last Reviewed Date: December 5, 2025	Revision History: 12/1/18; 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes may only use or disclose protected health information (PHI) for marketing purposes in accordance with the procedures set forth below.

Substance Use Disorder Information shall only be disclosed in accordance with Chimes' "Use and Disclosure of Substance Use Disorder Information" policies (P012 and subparts). Psychotherapy notes, SUD Counseling notes and mental health records shall only be disclosed in accordance with Chimes' "Use and Disclosure of PHI – Psychotherapy Note & SUD Counseling Notes" policy (P013.01).

PROCEDURES

I. General Procedures

A. Except as permitted below, workforce members shall not use or disclose PHI in connection with marketing communications without first obtaining a valid HIPAA authorization from the individual who is the subject of the PHI.

B. Workforce members shall direct all questions to the Privacy Official.

II. Approval Procedures

A. All materials; brochures; publications; patient education or instructional materials; and intranet, social media and website content for distribution to employees, patients, outside organizations or agencies, volunteers, or the general public, whether in print, digital form, or broadcast, must be approved by the Privacy Official in accordance with this Policy and applicable law.

B. Prior to commencing any use of PHI that may qualify as "marketing," workforce members shall consult the Privacy Official, who shall consult legal counsel to ensure compliance with legal requirements, including assessing whether an authorization is required.

1. The Privacy Official will assess whether the proposed communication encourages recipients to purchase or use a product or service;

2. The Privacy Official will confirm that either:

i. The communication meets one of the exceptions to the marketing authorization requirement set forth below; or

ii. Chimes has obtained a valid authorization pursuant to Chimes' "Authorizations for Uses and Disclosures" policy (P007).

C. Authorization Not Required.

1. The Privacy Official may approve the following marketing communications without a valid authorization:

i. *Promotional Gift of Nominal Value*. Chimes may make a marketing communication in the form of a promotional gift of nominal value if the Compliance Officer approves the gift.

ii. *Face-to-Face Communication*. Chimes may make a marketing communication in the form of a face-to-face communication to an individual.

D. Activities That Are Not "Marketing" under HIPAA

1. With the approval of the Privacy Official and so long as Chimes does not receive any financial remuneration in exchange for making the communication, the following types of communications are not "marketing":

i. Communications made for treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;

ii. Communications made for purposes of case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions;

iii. Communications made to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication

2. Communications made to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual are not marketing so long as any financial remuneration received by Chimes in exchange for making the communication is reasonably related to Chimes' cost of making the communication.

REGULATORY REFERENCES

45 CFR § 164.501

45 CFR § 508(a)(3)

Chimes Privacy Policies & Procedures	
Title: Uses and Disclosures of PHI – Research	**No. P013.11**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes may only use or disclose protected health information (PHI) for research purposes in accordance with the procedures set forth below. Research is defined in the Privacy Rule as, "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."

Substance Use Disorder Information shall only be disclosed in accordance with Chimes' "Use and Disclosure of Substance Use Disorder Information" policies (P012 and subparts). Psychotherapy notes, SUD Counseling notes and mental health records shall only be disclosed in accordance with Chimes' "Use and Disclosure of PHI – Psychotherapy Note & SUD Counseling Notes" policy (P013.01).

PROCEDURES

I. General Procedures. With respect to "research" as such term is defined by HIPAA, Chimes shall ensure the following:

A. Chimes does not use or disclose PHI for research purposes unless all of the requirements of the Privacy Rule have been met including approval by an Institutional Review Board or privacy board, reviews preparatory to research, review and approval procedures, and required signatures.

B. All questions shall be directed to the Privacy Official.

II. Required Approvals and Representations. Prior to using or disclosing PHI for research, the Privacy Official will ensure that Chimes:

A. Obtains documentation that an alteration to or waiver, in whole or in part, of the individual's authorization has been approved by:

1. An Institutional Review Board established under applicable law; or

2. A privacy board that:

i. Has members with varying backgrounds and appropriate professional competency as is needed to review the effect of the research protocol on the individual's privacy rights and related interests;

ii. Includes at least one member who is (a) not affiliated with Chimes, (b) not affiliated with the entity conducting or sponsoring the research, and (c) not related to any person who is affiliated with Chimes or the entity conducting or sponsoring the research.

iii. Does not have any member participating in a review in which the member has a conflict of interest.

B. Obtains the following representations from the researcher:

1. That uses and disclosures are sought solely to review PHI as needed to prepare a research protocol or for similar preparatory to research;

2. That no PHI is to be removed from Chimes by the researcher; and

3. That PHI for which use or access is sought is for research purposes.

C. Obtains, with respect to decedents, the following from the researcher:

1. A representation that the use or disclosure sought is solely for research on the PHI or decedents;

2. Documentation of the death of the individual; and

3. A representation that the PHI for which use or disclosure is sought is necessary for the research purposes.

III. Uses and Disclosures. Chimes may use or disclose PHI based upon documentation of approval of an alteration or wavier if the Privacy Official ensures, prior to any use or disclosure, that the documentation includes:

A. The identity of the IRB or Privacy Board approving the waiver or alteration;

B. The date of the approval of the waiver or alteration;

C. A statement that the following criteria for the waiver or alteration have been met:

1. The use or disclosure of PHI involves no more than minimal risk to the individuals or their privacy, based on:

i. An adequate plan to protect identifiers from improper use and disclosure;

ii. An adequate plan to destroy the identifiers at the earliest opportunity (unless there is a health or research justification for retaining identifiers or such retention is otherwise Required By Law); and

iii. Adequate assurances that the PHI will not be reused or disclosed

to any other person or entity except as required by law, for authorized oversight of the research project, or for other research permitted under this policy.

2. The research could not practicably be conducted without the alteration or waiver; and

3. The research could not practicably be conducted without access to and use of the PHI.

D. A brief description of the PHI to be used or disclosed;

E. A statement that the alteration or waiver of authorization has been reviewed and approved by the IRB or Privacy Board in accordance with normal or expedited procedures under the privacy standards.

1. The IRB is required to follow the requirements of the Common Rule (45 CFR Part 46, Subpart A), including the normal review procedures or the expedited review procedures.

2. A privacy board must:

i. Review the proposed research at a convened meeting at which a majority of the privacy board members are present, including at least one member who is sufficiently independent of Chimes and the entity conducting or sponsoring the research, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present; and

ii. Use an expedited review procedure, but only if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the PHI for which use or disclosure is being sought, in which the review and approval of the alteration or waive of authorization is carried out by the chair of the privacy board, or by one or more members of the privacy board as designed by the chair.

F. The signature of the Chair or other member, as designated by the Chair, of the IRB or Privacy Board.

REGULATORY REFERENCES

45 CFR § 164.512(i)(1)
45 CFR § 164.512(i)(2)

Chimes Privacy Policies & Procedures	
Title: Data Aggregation	**No. P014**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes may only engage in Data Aggregation with respect to PHI that it creates, receives, or maintains as a Covered Entity. With respect to PHI created, received, or maintained when acting as a Business Associate, Chimes may only engage in Data Aggregation to the extent permitted under the terms of applicable services agreements and Business Associate Agreement(s).

PROCEDURES

I. General Procedures.

A. Chimes may engage in Data Aggregation with respect to PHI that it creates, receives, or maintains as a Covered Entity for health care operations purposes.

B. If acting as a Business Associate, Chimes may engage in Data Aggregation of PHI created, received, maintained or transmitted on behalf of multiple clients only to the extent that each client has expressly authorized Data Aggregation as a permissible Use by Chimes on behalf of the respective client. Data Aggregation services shall be related to the health care operations of the covered entities for which it has agreements.

C. Any request for Data Aggregation services shall be sent to the Privacy Official for review to ensure compliance with legal requirements.

II. Questions. Any questions should be directed to the Privacy Official.

REGULATORY REFERENCES

45 CFR § 164.501
45 CFR § 164.504

Chimes Privacy Policies & Procedures	
Title: Responding to Requests from Third Parties	**No. P015**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

This policy outlines the procedures Chimes ("Chimes") follows when it receives a request for medical records from a third-party.

PROCEDURES

I. **Application of Policy**. In responding to requests from third parties, Chimes shall take the following steps:

A. Workforce members who receive a request for PHI from a third party shall promptly send such request to the Privacy Official, who will address the request directly.

B. The Privacy Official shall ensure that he or she reasonably determines the identification and authority of any individual requesting PHI, pursuant to Chimes' "Verification" policy (P009).

1. Requests for PHI of Deceased Individuals.

i. Chimes may receive requests from a decedent's family members, executor, administrator, probate personal representative, legal guardian, conservator or other person. Chimes' obligation to protect the confidentiality of PHI does not lapse until 50 years after the death of the individual. Presentation of a death certificate alone is not sufficient to allow Chimes to disclose a deceased patient's PHI.

ii. If the individual is deceased, Chimes may disclose to a family member, other relative, a close personal friend of the individual, a personal representative of the individual, another person who was responsible for the care of the individual, or any other persons that was identified by the individual who were involved in the individual's care or payment for health care prior to the individual's death, PHI of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the deceased individual that is known to Chimes.

iii. Financial powers of attorney and durable powers of attorney for health care terminate at the death of the patient. Therefore, workforce members shall not disclose or release PHI pursuant to a

power of attorney or durable power of attorney for health care unless such person is court appointed as the patient's executor, administrator, or probate personal representative.

iv. Legal guardianships and conservatorships terminate at the death of the patient. Therefore, workforce members shall not disclose or release PHI to the legal guardian of person or property, or conservator of a deceased patient unless such person is court appointed as the patient's executor, administrator, or probate personal representative.

v. Persons who present a court order and letters testamentary or letters of administration that appoint that person as the executor, administrator, or probate personal representative of a decedent's estate will be treated as a probate personal representative for purposes of requesting and receiving PHI.

vi. Workforce members may disclose PHI to family members of the decedent and others who were involved in the care or payment for care of the decedent prior to death, unless doing so is inconsistent with any prior expressed preference of the decedent that is known to Chimes.

vii. Chimes will disclose only de-identified information to researchers who request PHI of deceased individuals and will not in any circumstances provide researchers with access to a deceased person's PHI.

C. Workforce members shall comply with Chimes' "Minimum Necessary" policy (P010).

D. Workforce members shall refer to Chimes' Use and Disclosure policies, HIPAA, and applicable state laws.

1. P013.01 – Uses and Disclosures of PHI – Psychotherapy Notes

i. Any request for mental health records or psychotherapy notes will be sent immediately to the Privacy Official who shall consult with legal counsel.

2. P013.02 – Uses and Disclosures of PHI – Treatment, Payment, Healthcare Operations

3. P013.03 – Uses and Disclosures of PHI – Law Enforcement

i. If Chimes receives a request from law enforcement, the Privacy Official shall consult with t legal counsel in order to ensure that

Chimes does not violate HIPAA or other applicable federal or state privacy laws.

ii. All requests for PHI from domestic and foreign military authorities will be sent to legal counsel immediately.

iii. Any request for PHI received from a federal official shall be forwarded immediately to the Privacy Official, who shall contact legal counsel.

4. P013.04 – Uses and Disclosures of PHI – Abuse, Neglect, and Domestic Violence

5. P013.05 – Uses and Disclosures of PHI – Judicial and Administrative Proceedings

i. All requests from courts, administrative tribunals, and attorneys shall be sent immediately to the Privacy Official, who shall consult with legal counsel.

6. P013.06 – Uses and Disclosures of PHI – Public Health

i. If Chimes receives a request or subpoena from a disaster relief organization, a public health authority, a coroner, a medical examiner, a funeral director, or a correctional institution, the Privacy Official shall consult with the Corporate Privacy Official and legal counsel to ensure that Chimes does not violate HIPAA or other applicable federal or state privacy laws.

ii. All requests for PHI from health care oversight agencies shall be immediately sent to the Privacy Official, who shall consult with legal counsel. Health care oversight agencies include the U.S. Department of Health and Human Services or other agencies authorized by law to conduct audits; civil, administrative or criminal investigations; inspections; licensure, and disciplinary actions; civil, administrative or criminal proceedings; or other activities for oversight of the health care system.

iii. Chimes is required to disclose PHI to the Secretary of the U.S. Department of Health & Human Services or, the Secretary's designee, when the Secretary is investigating or auditing Chimes to determine its compliance with HIPAA and other applicable state and federal laws and regulations. Legal counsel shall be consulted.

7. P013.07 – Uses and Disclosures of PHI – Persons Involved in Care; Notification; Facility Directory

8. P013.08 – Uses and Disclosures of PHI – De-Identification of PHI and Limited Data Sets

9. P013.09 – Uses and Disclosures of PHI – Fundraising

10. P013.10 – Uses and Disclosures of PHI – Marketing

11. P013.11 – Uses and Disclosures of PHI – Research

E. Disclosures made pursuant to this policy are to be tracked in accordance with the "Tracking and Accounting of Disclosures" policy (P021), and may be subject to a request for accounting from an individual. Records of disclosures should be kept for at least six (6) years after the disclosure is made.

REGULATORY REFERENCES

45 CFR § 164.502(i)
45 CFR § 164.508(a)(4)
45 CFR § 164.512(a)

Chimes Privacy Policies & Procedures	
Title: Mitigation of Unauthorized Uses and Disclosures	**No. P016**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

If a workforce member, Business Associate, or any other third party uses or discloses PHI in an unauthorized manner, Chimes will mitigate, to the extent practicable, any harmful effects of which it is aware.

PROCEDURES

I. Chimes shall mitigate, to the extent practicable, any harmful effect that is known to Chimes, arising from a use or disclosure of PHI that was in violation of Chimes' policies and procedures or applicable law.

A. Workforce members shall report any information regarding an unauthorized use or disclosure of PHI to the Privacy Official.

B. Where applicable, mitigation may include reporting any use or disclosure of PHI not provided for by the business associate agreement and any security incident of which Chimes becomes aware to the covered entity; and documenting such disclosures of PHI and information related to such disclosures as would be required for the covered entity to respond to a request for an accounting of disclosure of PHI in accordance with HIPAA.

C. The Privacy Official shall determine how best to mitigate any known harmful effects of the violation. The Privacy Official will consider:

1. Identifying the source(s) of the disclosure and taking appropriate corrective action;

2. Contacting the recipient of the information that was the subject of the unauthorized disclosure and requesting that such recipient either destroy or return the information;

3. Instructing such recipient to make no further disclosures of such information;

4. Reviewing, and correcting where appropriate, any policy or procedure of Chimes that directly caused or contributed to the unauthorized use or disclosure;

5. Implementing additional safeguards to mitigate the risk of similar unauthorized uses and disclosures;

6. Providing training to workforce members involved in or responsible for the unauthorized use or disclosure;

7. Including the unauthorized use or disclosure in Chimes' accountable disclosure log in accordance with the "Tracking and Accounting of Disclosures" policy (P021);

8. Depending on the circumstances, notifying the individual whose PHI was the subject of the unauthorized use or disclosure; and/or

9. Offering credit monitoring to the individual(s) whose PHI was the subject of the unauthorized use or disclosure if the unauthorized use or disclosure involves an individual's Social Security Number, health plan identification number, credit/debit card number or other financial account information.

D. The Privacy Official will coordinate with and require business associates to mitigate, to the extent possible, harmful effects from unauthorized uses or disclosures of PHI known to and/or caused by them.

E. Please note, effective April 16, 2024 and forward the same mitigation, breach notification and reporting obligations which apply under HIPAA also apply to substance use disorder treatment records under 42 CFR Part 2.

REGULATORY REFERENCES

45 CFR § 164.530(f)

42 CFR § 2.16

Chimes Privacy Policies & Procedures	
Title: Notice of Privacy Practices	**No. P017**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes has developed and shall maintain a Notice of Privacy Practices (NOPP). All individuals receiving treatment from Chimes shall be provided the NOPP, which includes information regarding the privacy policies and procedures of Chimes, the uses and disclosures of protected health information (PHI), and individual rights. The NOPP will also be prominently posted in the registration area at Chimes.

Chimes shall not use or disclose PHI in a manner that is inconsistent with its Notice of Privacy Practices.

PROCEDURES

I. Content of the Notice.

A. The NOPP shall be written in plain language and include all HIPAA required elements described in 45 CFR § 164.520(b) and 42 CFR § 2.22.

B. The Privacy Official shall ensure that the NOPP contains descriptions in sufficient detail to inform patients of the uses and disclosures of PHI that are permitted or required by the Health Insurance Portability and Accountability Act (HIPAA) and other applicable laws.

C. The NOPP will be translated into languages other than English when determined necessary to provide reasonable access for patients with limited English proficiency, in accordance with HHS Office for Civil Rights guidance.

II. Delivery of the Notice.

A. Upon Admission. Chimes provides the NOPP, electronically or hard copy, no later than the date of the first service delivery, including service delivered electronically.

1. Each new patient will receive a copy of the NOPP at the time of admission and will be asked to sign an Acknowledgement of Receipt of the Notice of Privacy Practices, indicating a copy of the NOPP was provided.

2. In an emergency treatment situation, Chimes provides the NOPP as soon as reasonably practicable after the emergency treatment situation.

B. Upon Request. Chimes makes its NOPP available upon request to any person.

1. All requests for a copy of the NOPP shall be responded to as soon as practicable.

2. For such requests, the NOPP shall be provided either in person in hard copy or by first class mail.

3. The NOPP may not be provided via email unless the individual or his/her personal representative specifically requests the NOPP via email, or consent to deliver via email has been obtained.

C. Onsite.

1. Chimes makes the NOPP available at its locations for individuals to take with them upon request.

2. Chimes posts the NOPP in a clear and prominent location where it is reasonable to expect individuals seeking service from Chimes to be able to read the NOPP. Typically, the NOPP will be prominently posted in the reception area of Chimes.

D. Electronically.

1. *Website*. A copy of the current NOPP shall be posted on the Chimes website.

i. The Privacy Official shall ensure that Chimes prominently posts its NOPP on its website and make the Notice available electronically through the website.

ii. The Privacy Official shall coordinate the NOPP with Chimes' website privacy policy and terms of use.

iii. The NOPP shall be posted in such a manner that it can be easily downloaded in a readable format.

2. *Email*. Chimes may provide a copy of the NOPP to a patient by email, if the patient has executed paperwork indicating email as an acceptable method of communication and such agreement has not been withdrawn.

i. If Chimes knows that the email transmission has failed, Chimes will provide a paper copy of the NOPP to the individual either in person or by first-class mail.

3. If the first service delivery to a patient is delivered electronically, Chimes must provide electronic notice automatically and contemporaneously in response to the patient's first request for service.

4. The individual who is the recipient of electronic notice may obtain a paper copy of the Notice from Chimes upon request.

III. Changes to the Notice.

A. Chimes will promptly revise, post revisions on the website as soon as possible, and distribute its Notice whenever there is a material change to the uses or disclosures, the individual's rights, Chimes' legal duties, or other privacy practices stated in the NOPP.

1. The Privacy Official must approve any and all changes to the NOPP.

2. If the NOPP permits Chimes to make changes to its terms at any time, a material change to the NOPP may be implemented at any time.

3. If the NOPP does not permit changes at any time, a material change to the NOPP will not be implemented prior to the effective date of the NOPP in which such material change is reflected.

B. If a change is made, the Privacy Official shall ensure that the new NOPP is distributed, prominently posted at any physical location in which individuals are seen, and that Chimes' website is updated.

C. The NOPP shall always contain an effective date which assists in the determination of the last time the NOPP was changed.

IV. Record Retention. Chimes shall retain copies of the Notices it issues and any written acknowledgments of receipt of the Notice (or documentation of good faith efforts to obtain such acknowledgment) for a period of six years from the date of their creation, or the date when such Notice last was in effect, whichever is later.

REGULATORY REFERENCES

45 CFR § 164.520(a)(1)
45 CFR § 164.520(b)(1)
45 CFR § 164.520(c)(2)
45 CFR § 164.520(c)(3)
45 CFR § 164.520(d)
45 CFR § 164.520(e)
42 CFR § 2.22

Chimes Privacy Policies & Procedures	
Title: Designated Record Set	**No. P018**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

A "Designated Record Set" is the group of records maintained by or for Chimes that is (i) the medical records and billing records about individuals maintained by or for Chimes, (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for Chimes to make decisions about individuals.

As used herein, the term "record" means any item, collection, or grouping of information that includes protected health information (PHI) and is maintained, collected, used, or disseminated by or for the covered entity.

PROCEDURES

I. **Designated Record Sets**. Chimes maintains the following Designated Record Sets containing Protected Health Information about patients:

A. Medical records;

B. Billing records;

C. Other records used, in whole or in part, by or for Chimes to make decisions about patients.

II. The Designated Record Set shall include the following items (if they exist):

A. Inpatient/Outpatient Medical Records, as follows:

1. Patient face sheet;

2. Authorization/Consent forms;

3. Intake forms signed by the patient or an authorized representative;

4. Advanced Directives;

5. Physician/non-physician practitioner orders or prescriptions;

6. Laboratory/pathology reports;

7. Imaging/Radiology reports;

8. History and physical examination reports;

9. Consultation reports;

10. Progress notes;

11. Nursing notes/assessments;

12. Medication administration records;

13. Results of any special tests or treatments;

14. Records obtained from other health care providers and used to make health care decisions;

15. Discharge summary reports;

16. Patient education records/discharge instructions;

17. Transfer forms; and

18. Source data not interpreted or summarized in the medical record.

B. Billing/Financial Records, as follows:

1. Insurance information;

2. Detailed bills;

3. Records of payments;

4. Adjustments;

5. Advanced Beneficiary Notices;

6. Eligibility Information; and

7. Coding summary.

C. Other records used to make decisions about patients, as follows:

1. Audiotapes not transcribed;

2. Videos/photographs of patients; and

3. Records maintained by a business associate/qualified service organization on behalf of Chimes that are not merely duplicates of information maintained by the facility.

III. The Designated Record Set shall <u>not</u> include the following items:

A. Psychotherapy Notes;

B. Data collected and maintained for peer review purposes;

C. Data collected and maintained for performance improvement purposes;

D. Data collected and maintained for compliance purposes;

E. Data collected and maintained for quality control purposes;

F. Risk management records;

G. Incident reports;

H. Infection control reports;

I. Administrative, attorney-client privileged, and any other protected reports;

J. Temporary notes or worksheets, reminders, and concurrent coding worksheets;

K. Incomplete record coversheets, clarification notes to/from physicians, etc.;

L. Source Data interpreted or summarized in the individual's medical record.

REGULATORY REFERENCES

45 CFR § 164.501

Chimes Privacy Policies & Procedures	
Title: Access to PHI	**No. P019**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: **December 5, 2025**	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes provides access to Protected Health Information (PHI) so long as the information or record is maintained by Chimes in the patient's "Designated Record Set" as defined by HIPAA.

PROCEDURES

I. **Right of Access**. Individuals have a right of access to review and obtain a copy of the PHI about the individual maintained in a Designated Record Set for as long as the PHI is maintained in the Designated Record Set.

A. The Designated Record Set is the group of records, which include (1) medical and billing records about individuals maintained by or for a covered health care provider (2) the enrollment, payment claims adjudication, and case or medical management record systems maintained by or for a health plan; or (3) is used in whole or in part, by or for a covered entity to make decisions about individuals. Please see Chimes' "Designated Record Set" policy (P018).

II. **Contact for Access Requests**. The Privacy Official, or his/her designee, shall serve as the point of contact responsible for receiving and processing all requests for access to PHI in a designated record set. The Privacy Official may consult with legal counsel as needed.

III. **Form of Requests**. All requests should be submitted in writing, and the individual receiving the request shall inform any requestor of this requirement. If unable to provide the request in writing, the staff member obtaining the oral request will document in writing the requested information.

A. Individuals shall be provided an appropriate written form upon request; however, requests do not need to be on Chimes' standard form. Other similar forms including the same specificity of the request may be used. If the individual is missing key information, he or she may be asked to complete the form or provide clarification.

B. Workforce members who are also "individuals" for purposes of the Privacy Rule, including those persons who are Chimes patients and personal representatives of Chimes patients, shall not access or attempt to access their own PHI through Chimes' health records or any information system that is not accessible to non-workforce members.

IV. **Response**.

A. Requests should be submitted in writing and forwarded immediately to the Privacy Official, who may consult with legal counsel as needed.

B. Timing. Chimes must act on all requests for access or inspection as soon as is practicable, and in no event more than 30 days after receiving the request, by either sending a denial letter or by providing the requested access to the records along with an invoice, if applicable. See subsection 2 below with respect to state law timing requirements.

1. If Chimes is unable to take action within the initial 30 days, it may extend the response time by no more than thirty (30) days, if Chimes sends the individual a written notice, *within the initial time period for the response*, that includes the reasons for the delay and the date by which Chimes will act on the request. Chimes may only extend the time period for the response once.

2. If an applicable state law requires a shorter response period, Chimes will comply with the time frame provided in such state law.

    i. The Privacy Official shall be responsible for identifying other state laws which might necessitate a shorter time period to respond.

C. Responsibility. The Privacy Official will prepare the response with the assistance of legal counsel as needed.

1. The Privacy Official may take one of the following actions on a request:

    i. Determine that the individual has no right of access (*e.g.* for (1) psychotherapy notes; and (2) information compiled for use in a criminal, civil, or administrative proceeding or action)

    ii. Provide access in accordance with this Policy;

    iii. Deny the request, without an opportunity for review; or

    iv. Deny the request and give the individual an opportunity to obtain review of the denial.

2. The Privacy Official shall contact all relevant business associates as necessary.

3. *Verification*. The Privacy Official shall verify any party requesting access, to PHI pursuant to Chimes' "Verification" policy (P009) before any action is taken.

D. Providing Access. The Privacy Official will notify the individual and arrange for a mutually convenient time and place to provide the access requested.

1. Chimes will provide the individual with copies of the Designated Record Set in one of the following forms:

i. The form and format that the individual requests, if the information is readily producible in that form; or, if not, in a readable hard copy form or such other form and format as agreed to by Chimes and the individual.

ii. If the PHI is maintained in one or more Designated Record Sets electronically and if the individual requests an electronic copy of such information, Chimes will provide the individual with access to the PHI in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by Chimes and the individual.

2. If an individual asks Chimes to transmit a copy of PHI directly to another person (instead of to the individual), Chimes must provide the copy to the designated person. An individual's request to transmit a copy of PHI to another person must be in writing, signed by the individual, clearly identify the person to whom the PHI is to be sent, and clearly identify where the PHI is to be sent.

i. If the PHI requested is located outside of Chimes' electronic health record, the individual making the request must complete an authorization that includes the required elements outlined in Chimes' "Authorizations Policy" (P007).

ii. If the PHI is located within Chimes' electronic health record, an individual's request to transmit a copy of PHI to another person must be in writing, signed by the individual, clearly identify the person to whom the PHI is to be sent, and clearly identify where the PHI is to be sent.

iii. Chimes may charge a fee for providing PHI directly to a third party at the request of an individual, and such fees are not limited to the reasonable, cost-based fees set forth in Section IV.D.4. of this Policy, below.

3. *Summary*. Chimes may provide the individual with a summary of the PHI requested, in lieu of providing access, if the individual agrees in advance to (i) the provision of the summary, and (ii) any reasonable, cost-based fees imposed by Chimes for such summary.

4. *Cost-Based Copying Charges*. Under HIPAA, when an individual makes a request for access to his/her own records, Chimes may only charge reasonable, cost-based fees to produce a copy of the Designated Record Set (copying, postage, and preparation of a summary (if the individual has agreed to a summary)). Such fees must also be permitted under state law. The Privacy Official or his/her designee shall determine and document the applicable fee schedule, which shall be reviewed no less than annually. For

operational procedure, refer to Standard Operating Procedure: Medical Records Copying Charges.

E. Denying Access. Unless otherwise prohibited by applicable law, Chimes may deny (in whole or in part) the individual access to his or her Designated Record Set as permitted by HIPAA.

1. If Chimes denies an individual access to certain information within that individual's record, Chimes shall grant, to the extent possible, access to all other requested information.

2. The Privacy Official shall consider applicable state law with legal counsel before denying an access request.

3. *Unreviewable denial*. Chimes shall deny individual access to the following types of information without an opportunity for review:

i. If the PHI is excepted from the right of access (Psychotherapy notes and information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding);

ii. If Chimes is acting under the direction of a correctional institution, an inmate makes a request, and the request would jeopardize the health, safety, security, custody, or rehabilitation of the inmates or the safety of any officer, employee, or other person at the institution or responsible for transporting of the inmate;

iii. An individual's access to PHI created or obtained by Chimes in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that (1) the individual has agreed to the denial of access when consenting to participate in the research that includes treatment and (2) Chimes has informed the individual that the right of access will be reinstated upon completion of the research.

iv. Any records subject to the Privacy Act, 5 USC § 552a, if the denial also meets the requirements of the Privacy Act.

v. If the PHI was obtained by someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

4. *Reviewable denial*: Chimes may deny individual access to or copies of the following types of information provided that the individual is given a right to have any such denial reviewed:

i. When a licensed health care professional has determined, in the exercise of professional judgment, that:

a. The access requested by the individual or their personal representative is reasonably likely to endanger the life or physical safety of the individual or another person (such as instances of abuse); or

b. The information requested makes reference to another person (other than a health care provider) and the access requested is reasonably likely to cause substantial harm to such other person. Harm may include physical or psychological harm; or

c. The request is made by the individual's personal representative and providing the requested access is reasonably likely to cause substantial harm to the patient or another person.

ii. In the above instances, the individual does have the right to appeal the denial.

5. *Notice of Denial*. If Chimes denies access, the Privacy Official shall provide a written notice of denial.

i. Written denial notices shall be written in plain language and include the following information:

a. Basis for the denial;

b. If applicable, a statement of the individual's right to request a review of a denial, including a description of how the individual may exercise such review rights;

c. A statement explaining how the individual may complain to Chimes by contacting the Privacy Official (including his or her telephone number) or complain to the Secretary of the Department of Health and Human Services; and

d. If access is denied because Chimes does not maintain the information, Chimes shall inform the individual of the location of that information, if known.

6. *Reviewing Denials*.

i. When denials are subject to review, a licensed health care professional that did not participate in the original decision to deny access shall perform the review. The referral for review must be prompt, and the reviewer must complete the review within a reasonable period of time.

ii. The reviewer will determine whether or not to deny access. The decision of the reviewer is final and is binding on Chimes.

iii. The Privacy Official will promptly provide written notice of the reviewer's decision to the individual and take steps to carry out the reviewer's decision. If the determination was to approve access, the Privacy Official, or his or her designee, will grant access.

V. Record Retention.

A. All requests and associated responses regarding access requests to PHI shall be documented and retained for a period of no less than six (6) years.

B. The titles of the persons or offices responsible for receiving and processing requests for access shall be documented and retained for a period of six (6) years.

C. The designated record sets that are subject to access by individuals shall be retained for a period of at least six (6) years.

REGULATORY REFERENCES

45 CFR § 164.524(a)(1)
45 CFR § 164.524(a)(2)
45 CFR § 164.524(a)(3)
45 CFR § 164.524(a)(4)
45 CFR § 164.524(b)(1)
45 CFR § 164.524(b)(2)
45 CFR § 164.524(c)(2)
45 CFR § 164.524(c)(3)
45 CFR § 164.524(c)(4)
45 CFR § 164.524(d)(1)
45 CFR § 164.524(d)(2)
45 CFR § 164.524(d)(3)
45 CFR § 164.524(d)(4)
45 CFR § 164.524(e)

Chimes Privacy Policies & Procedures	
Title: Amendment to PHI	**No. P020**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes shall respond to requests for amendment of protected health information (PHI) maintained in a Designated Record Set as outlined in this policy.

PROCEDURES

I. Right to Request Amendments. An individual has the right to have Chimes amend PHI about the individual in a Designated Record Set for as long as the PHI is maintained in the Designated Record Set.

II. Contact for Amendment Requests. The Privacy Official, or his/her designee, shall serve as the point of contact responsible for receiving and processing all formal requests for amendment to PHI in a Designated Record Set.

III. Form of Requests. All requests should be submitted in writing, and the individual receiving the request shall inform individuals of this requirement.

A. The individual shall include a reason to support the requested amendment.

B. Individuals shall be provided an appropriate written form upon request; however, requests do not need to be on Chimes' standard form. Other similar forms with the same specificity of the request may be used. If the individual is missing key information, he or she may be asked to complete the form.

C. Workforce members who are also "individuals" for purposes of the Privacy Rule, including those persons who are Chimes patients and personal representatives of Chimes patients, shall not amend or attempt to amend their own PHI through Chimes' electronic health record or other information system that is not accessible to non-workforce members.

IV. Response.

A. Requests should be submitted in writing and forwarded immediately to the Privacy Official, or his/her designee.

B. Timing. Chimes must either accept or deny an individual's request for amendment as soon as is practicable, and in any event within sixty (60) days of receiving the request.

1. If Chimes is unable to take action within the initial sixty (60) days, it may extend the response time by no more than thirty (30) days, if Chimes sends the individual a written notice, *within the initial time period for the*

response, that includes the reasons for the delay and the date by which Chimes will act on the request. Chimes may only extend the time period for the response once.

2. If an applicable state law requires a shorter response period, Chimes will comply with the time frame provided in such state law.

    i. The Privacy Official shall be responsible for identifying state laws which might necessitate a shorter time period to respond.

C. Responsibility. The Privacy Official, or his/her designee, will prepare the response.

1. The Privacy Official, in consultation with legal counsel as needed, may take one of the following actions on a request:

    i. Make the requested amendment; or

    ii. Deny the requested amendment.

2. The Privacy Official shall contact all relevant business associates as necessary.

3. *Verification*. The Privacy Official shall verify any party requesting access, to PHI pursuant to Chimes' "Verification" policy (P009) before any action is taken.

D. Making the Amendment.

1. The Privacy Official, or his/her designee, shall make the requested amendment if all the following conditions are met:

    i. The request is written, clearly states a reason for the amendment, and includes any necessary supporting information;

    ii. The information to be amended is maintained and controlled by Chimes;

    iii. The information is maintained as a part of the individual's Designated Record Set;

    iv. The individual has the right to access the PHI; and

    v. Chimes considers the amendment necessary for the PHI to be accurate and complete.

2. If Chimes accepts the requested amendment, in whole or in part, the Privacy Official, or his/her designee, shall:

i. Make the appropriate amendment to the PHI that is the subject of the request for amendment by, at a minimum, identifying the records in the Designated Record Set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment;

ii. Promptly inform the individual that the amendment has been accepted and obtain the individual's identification of an agreement to have Chimes notify the relevant persons with which the amendment needs to be shared;

iii. Make reasonable efforts to inform and provide the amendment within a reasonable period of time to:

a. Persons identified by the individual as having received PHI about the individual and requiring the amendment; and

b. Persons, including business associates, that Chimes knows have the PHI that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

E. Denying the Amendment.

1. Chimes may deny an individual's request for amendment, if the Privacy Official determines that the PHI that is the subject of the request:

i. Was not created by Chimes, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;

ii. Is not part of the Designated Record Set;

iii. Would not be available under Chimes' "Access to PHI" policy (P019); or

iv. Is accurate and complete.

2. If Chimes denies the amendment in whole or in part, the Privacy Official shall undertake the following:

i. *Written Statement*. The Privacy Official shall provide the individual who requested the amendment with a written denial as soon as is practicable, and in no event later than sixty (60) days after receiving the request. The denial shall be written in plain language and state:

a. The basis for the denial;

b. A statement of the individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

c. A statement that, if the individual does not submit a statement of disagreement, the individual may request that Chimes provide the individual's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment; and

d. A description of how the individual may complain to Chimes or to the Secretary, Office for Civil Rights of HHS. The description must include the telephone number of Chimes' Privacy Official.

ii. *Statement of Disagreement*. The Privacy Official shall ensure that Chimes permits the individual to submit a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement.

a. The Privacy Official, in consultation with legal counsel, may reasonably limit the length of a statement of disagreement.

iii. *Written Rebuttal*. The Privacy Official, in consultation with legal counsel, may prepare a written rebuttal to the statement of disagreement. Whenever a rebuttal is prepared, the Privacy Official shall provide a copy to the individual who submitted the statement of disagreement.

iv. *Recordkeeping*. The Privacy Official shall identify the PHI in the Designated Record Set that is the subject of the disputed amendment and append or otherwise link the individual's statement of disagreement, if any, and Chimes' written rebuttal, if any, to the Designated Record Set.

v. *Future Disclosures*. The Privacy Official shall ensure that:

a. If a statement of disagreement has been submitted by the individual, Chimes will include the material appended, or at the election of Chimes, an accurate summary of any such information, with any subsequent disclosure of the PHI to which the disagreement relates;

1. When a subsequent disclosure is made as part of a HIPAA standard transaction under 45 CFR Part 162 that does not permit the additional material to be included in the transaction, the Privacy Official may

separately disclose (or transmit electronically) the material required to the recipient

b. If the individual has not submitted a written statement of disagreement, Chimes must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the PHI only if the individual has requested such action.

V. Record Retention. All requests and associated responses regarding amendments to PHI shall be documented and retained for a period of no less than six (6) years

REGULATORY REFERENCES

45 CFR § 164.526(a)(1)
45 CFR § 164.526(a)(2)
45 CFR § 164.526(c)
45 CFR § 164.526(d)

Chimes Privacy Policies & Procedures	
Title: Tracking and Accounting of Disclosures	**No. P021**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes shall respond to requests for an accounting of disclosures of protected health information (PHI) as outlined in this policy.

PROCEDURES

I. Tracking Disclosures and the Right to an Accounting.

A. Right to an Accounting. An individual generally has a right to receive an accounting of certain disclosures of PHI made by Chimes and occurring in the six (6) years prior to the date on which the accounting is requested.

B. Tracking Disclosures. Disclosures of PHI for the following purposes will be documented by the Privacy Official. Such documentation shall include the information required to be provided for an accounting, as set forth below, and shall be retained for a period of at least six (6) years from the date of the disclosure:

1. Required by law;

2. Public health activities, including child abuse reporting; abuse, neglect, and domestic violence reporting; FDA reporting; communicable disease reporting; certain employment-related disclosures; disclosures to coroners/medical examiners; and disclosures for organ procurement purposes;

3. Health oversight activities;

4. Judicial and administrative proceedings, including in response to legal process;

5. Law enforcement purposes, including certain injury reporting;

6. In order to avert a serious threat to health or safety;

7. Specialized government functions (Military and veterans' activities & protective services for the President and others); and

8. Worker's compensation disclosures necessary to comply with laws relating to worker's compensation programs.

C. Exceptions. An individual does not have a right to an accounting, and Chimes does not track, disclosures for the following purposes:

1. To carry out treatment, payment, and health care operations (§ 164.506);

2. To individuals of PHI about them (§ 164.502);

3. Incident to a use or disclosure otherwise permitted or required (§ 164.502);

4. Pursuant to an authorization (§ 164.508);

5. For any facility's directory, to persons involved in the individual's care, or for other notification purposes (§ 164.510);

6. For national security or intelligence purposes (§ 164.512(k)(2));

7. To correctional institutions or law enforcement agencies (§ 164.512(k)(5));

8. As part of a limited data set (§ 164.514(e)); or

9. That occurred prior to the compliance date for Chimes.

D. Temporary Suspension of Right. Chimes is required to temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official for the time specified by such agency, if such agency or official:

1. Provides the Privacy Official with a written statement that:

   i. States that such an accounting to the individual would be reasonably likely to impede the agency's activities; and

   ii. Specifies the time for which such suspension is required.

2. Provides the Privacy Official an oral statement consistent with Subsection (1) above, provided that the Privacy Official shall:

   i. Document the statement, including the identity of the agency or official making the statement; and

   ii. Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is provided.

II. Contact Person for Accounting Requests. The Privacy Official shall serve as the point of contact responsible for receiving and processing all formal requests for accounting of disclosures of PHI.

III. Form of Request. All requests should be submitted in writing, and the individual receiving the request shall inform individuals of this requirement.

A. Individuals shall be provided an appropriate written form upon request; however, requests do not need to be on Chimes' standard form. Other similar forms with the same specificity of the request may be used. If the individual is missing key information, he or she may be asked to complete the form.

B. Workforce members who are also "individuals" for purposes of the Privacy Rule, including those persons who are Chimes patients and personal representatives of Chimes patients, shall not create accountings with respect to their own PHI through Chimes' health records or any other information system that is not accessible to non-workforce members.

IV. Response

A. Requests should be submitted in writing and forwarded immediately to the Privacy Official.

B. Timing. Chimes shall act on the individual's request for an accounting as soon as is practicable, and in any event no more than sixty (60) days after receiving the request.

1. If Chimes is unable to take action within the initial 60 days, it may extend the response time by no more than thirty (30) days, if Chimes sends the individual a written notice, within the initial time period for the response, that includes the reasons for the delay and the date by which Chimes will act on the request. Chimes may only extend the time period for the response once.

2. If an applicable state law requires a shorter response period, Chimes will comply with the time frame provided in such state law.

i. The Privacy Official shall be responsible for identifying state laws which might necessitate a shorter time period to respond.

C. Responsibility. The Privacy Official will prepare the response.

1. The Privacy Official shall contact all relevant business associates as necessary.

2. *Verification*. The Privacy Official shall verify any party requesting access, to PHI pursuant to Chimes' "Verification" policy (P009) before any action is taken.

D. Content of Response. The written accounting shall include the following with respect to disclosures of PHI that occurred during the six (6) years prior to the date of the request, including disclosures to or by business associates:

1. The date of the disclosure;

2. The name of the entity or person who received PHI and, if known, the address of such entity or person;

3. A brief description of the PHI disclosed (with relevant dates when possible); and

4. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or, in lieu of such statement, a copy of the written request for a disclosure (e.g., subpoena or court order).

5. *Exceptions for multiple disclosures*:

    i. If Chimes has made multiple disclosures of PHI to the same person or entity for a single purpose for treatment, payment, or health care operations purposes, the account may provide (1) the information required above for the first disclosure during the accounting period; (2) the frequency, periodicity, or number of the disclosures made during the accounting period; and (3) the date of the last such disclosure during the accounting period.

    ii. If Chimes has made multiple disclosures of PHI to the same person or entity for a single purpose for which an authorization is not required, the account may provide (1) the information required above for the first disclosure during the accounting period; (2) the frequency, periodicity, or number of the disclosures made during the accounting period; and (3) the date of the last such disclosure during the accounting period.

    iii. If Chimes has made multiple disclosures of PHI to the same person or entity for a particular research purpose for 50 or more individuals, the accounting may, with respect to such disclosures for which the PHI about the individual may have been included, provide:

        a. The name of the protocol or other research activity;

        b. A plain-language description of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

        c. A brief description of the type of PHI disclosed;

        d. The date or period of time during which the disclosures occurred;

        e. The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and

f. A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or other research activity.

g. Upon request from the individual, Chimes shall also assist in contacting the entity that sponsored the research and the researcher.

E. Fees. Chimes shall provide one (1) free accounting every twelve (12) months. If an individual requests another accounting within the same twelve (12) month time period, the Privacy Official may charge a reasonable cost-based fee to the individual for the costs of producing such accountings. Prior to charging a fee, the Privacy Official will inform the individual, in writing, of the fee and provide the individual with an opportunity to withdraw or modify the request.

V. Substance Use Disorder Information. Upon request, Chimes provides patients who have consented to disclose information using a general designation in an authorization a list of the individuals and entities to which their information has been disclosed pursuant to the general designation. Chimes tracks the information necessary to account for these disclosures and responds to requests for accountings of such disclosures in a timely fashion.

A. All requests for an accounting of disclosures of Substance Use Disorder Information shall be directed to and handled by the Privacy Official, who shall consult with legal counsel as needed.

B. Requests must be submitted in writing.

C. Chimes shall respond to requests for accountings of disclosures of Substance Use Disorder Information within thirty (30) days of receiving the request.

D. In response to the request for an accounting, Chimes shall provide the following to patients who have consented to disclose Substance Use Disorder Information using a general designation:

1. A list of the entities to which their information was disclosed pursuant to the general designation within the past three (3) years;

2. The date of each disclosure; and

3. A brief description of the patient identifying information disclosed.

E. Chimes tracks the information needed for the accounting pursuant to its "Substance Use Disorder Information – Uses and Disclosures with Authorization" policy (P012.01).

F. Responses to requests for accountings are documented and maintained by the Privacy Official.

VI. **Record Retention**. Disclosures required to be tracked and the related information, accountings provided under this Policy, and the titles of the persons responsible for receiving and processing requests under this Policy shall be documented and retained for a period of six (6) years.

REGULATORY REFERENCES

42 CFR § 2.13(d)
45 CFR § 164.528(a)
45 CFR § 164.528(b)
45 CFR § 164.528(c)
45 CFR § 164.528(d)

42 CFR § 2.25

Chimes Privacy Policies & Procedures	
Title: Requests for Restrictions and Confidential Communications	**No. P022**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes accommodates individuals' requests for restrictions on the use and disclosure of Protected Health Information (PHI) made for treatment, payment and health care operations purposes, or disclosures to family or others involved in a patient's care.

The Privacy Rule provides for the right to request to receive confidential communications of PHI by alternative means or at alternative locations. Chimes will accommodate all reasonable requests for confidential communications.

PROCEDURES

I. Rights to Request Restrictions and Confidential Communications. Individuals have the rights to:

A. Request that Chimes restrict the following:

1. Uses and disclosures of PHI about the individual to carry out treatment, payment and health care operations;

2. Permitted disclosures of PHI to the individual's family members, other relatives, close personal friends, and others identified by the individual;

3. Permitted disclosures to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death; and

4. Permitted disclosures to public or private entity authorized by law or by its charter to assist in disaster relief efforts.

B. Request to receive communications of PHI from Chimes by alternative means or at alternative locations.

II. Contact for Access Requests. The Privacy Official shall serve as the point of contact responsible for receiving and processing all formal requests for restrictions on the use or disclosure of PHI in a Designated Record Set.

III. Form of Requests. All requests should be submitted in writing, and the individual receiving the request shall inform individuals of this requirement.

A. Individuals shall be provided an appropriate written form upon request; however, requests do not need to be on Chimes' standard form. Other similar forms with specificity of the request may be used. If the individual is missing key information, he or she may be asked to complete the form.

1. Requests for restrictions should include the following:

i. A description of the information to be limited;

ii. Whether the limitation applies to uses, disclosures, or both; and

iii. A description of to whom the limitations would apply.

2. Requests regarding communications should include the following, when appropriate:

i. Information as to how payment, if any, will be handled; and

ii. Specification of an alternative address or other method of contact.

iii. Chimes will *not* require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

B. Workforce members who are also "individuals" for purposes of the Privacy Rule, including those persons who are Chimes patients and personal representatives of Chimes patients, shall not access or attempt to access their own PHI through Chimes' health records or other information system that is not accessible to non-workforce members.

IV. Response.

A. Requests should be submitted in writing and forwarded immediately to the Privacy Official.

B. Timing. Chimes shall act on the individual's request as soon as is practicable and in any event no more than sixty (60) days after receiving the request.

1. If an applicable state law requires a shorter response period, Chimes will comply with the time frame provided in such state law.

i. The Privacy Official shall be responsible for identifying other state laws which might necessitate a shorter time period to respond.

C. Responsibility. The Privacy Official will prepare the response.

1. The Privacy Official shall notify, in writing, the individual of Chimes' decision regarding the request. The request and the decision shall be noted in the patient's records.

2. The Privacy Official shall contact all relevant business associates as necessary.

3. *Verification*. The Privacy Official shall verify any party requesting access, to PHI pursuant to Chimes' "Verification" policy (P009) before any action is taken.

D. Confidential Communications. Chimes shall accommodate all reasonable requests by individuals to receive communications of PHI from Chimes by alternative means or at alternative locations.

E. Restrictions.

1. Chimes shall permit individuals to request restrictions with respect to the following:

i. Uses and disclosures of PHI about the individual to carry out treatment, payment and health care operations;

ii. Permitted disclosures of PHI to the individual's family members, other relatives, close personal friends, and others identified by the individual;

iii. Permitted disclosures to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death; and

iv. Permitted disclosures to a public or private entity that is authorized by law or by its charter to assist in disaster relief efforts.

2. *Response*. In response to such requests, Chimes shall:

i. Agree to, unless otherwise required by law, a request for restrictions on disclosures to a health plan for purpose of payment or health care operations, if the PHI pertains solely to a health care item or service for which the patient has paid, out of pocket, in full.

ii. Consider all other requests on a case-by-case basis, as Chimes is only required to honor the restriction set forth in (i) above. The Privacy Official shall consider Chimes' ability to meet the request prior to agreeing to the restriction.

3. *Compliance*. If Chimes agrees to a restriction, Chimes shall abide by the terms of the restriction, except in the following instances:

i. If the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment, workforce members may use the restricted PHI, or may disclose such PHI to a health care provider, to provide such treatment, but Chimes must request that such health care provider not further use or disclose the PHI;

ii. The PHI is required to be disclosed to the Secretary of U.S. Department of Health & Human Services for an investigation to determine compliance with the HIPAA Rules;

iii. When the Privacy Rule does not require Chimes to obtain the individual's authorization or to give the individual an opportunity to object (i.e., those uses and disclosures that are required by law, for public health activities, concerning victims of abuse, neglect, or domestic violence, for health oversight activities, for judicial and administrative proceedings, for law enforcement purposes, about decedents, to avert serious threat to health or safety, for specialized government functions or for workers' compensation purposes).

4. *Termination*. Chimes may terminate an agreed-upon restriction if:

i. The individual requests or agrees to the termination in writing;

ii. The individual orally agrees to the termination and the agreement is documented; or

iii. The restriction is not required, Chimes informs the individual that it is terminating the agreement for the restriction, and the termination is only effective with respect to PHI about the individual created or received after Chimes has so informed the patient.

iv. The Privacy Official shall fully document the termination of any restriction, including all applicable dates

V. Record Retention. All requests and associated response regarding restrictions to PHI shall be documented and retained for a period of six (6) years.

REGULATORY REFERENCES

45 CFR § 164.502(h)
45 CFR § 164.522(a)(1)
45 CFR § 164.522(a)(2)
45 CFR § 164.522(a)(3)
45 CFR § 164.522(b)(1)

Chimes Privacy Policies & Procedures	
Title: Business Associates and Qualified Service Organizations	**No. P023**
Responsible Party: Privacy Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

It is the policy of Chimes to ensure that all service providers and vendors that create, receive, maintain, or transmit protected health information (PHI) have executed a Business Associate Agreement prior to receiving access to such PHI. Chimes must enter into Business Associate Agreements when determined necessary and appropriate by the Privacy Official, and legal counsel.

Chimes should propose Chimes' template Business Associate Agreement. If a Business Associate requests use of its own form or requests revisions to Chimes' template, workforce members must refer the request to the Privacy Official, who may consult with legal counsel as needed.

PROCEDURES

I. General Procedures.

A. Determination

1. Prior to entering into any service contract with a service provider, the Privacy Official shall identify and determine whether the service provider is a Business Associate.

2. In case of a question as to whether a business associate agreement is necessary, the Privacy Official shall consult with legal counsel.

B. Diligence

1. At the discretion of the Privacy Official, potential business associates may be asked to permit inspection of their books, records, and policies related to compliance with HIPAA requirements.

2. At the discretion of the Privacy Official, potential business associates may also be asked to attest to their compliance with all HIPAA business associate requirements including, but not limited to, performance of a Security Rule required risk analysis and implementation of administrative, technical, and physical safeguards.

C. Standard Agreement

1. The Privacy Official shall maintain a "standard" business associate agreement that shall be presented to service providers or contractors who will or may have the potential to access any PHI.

    i. There may be different "standards" for different relationships.

    ii. The "standard" shall maintain all required terms and conditions as required by HIPAA.

2. As the "standard" may change from time to time, it is not attached to this policy, but shall be maintained by the Privacy Official.

D. Contracting

1. The business associate will either:

    i. Be provided with Chimes' standard business associate agreement; or

    ii. Provide a copy to Chimes of its standard business associate agreement.

2. If a modification is made to Chimes' standard agreement, or if Chimes is asked to execute the vendor's standard agreement, the documents will be referred to the Privacy Official, and legal counsel for review and response. Any standard agreement provided by a prospective vendor must include language required by 42 CFR Part 2.

E. The Privacy Official shall routinely review business associate relationships and contracts to ensure compliance with the requirement that all business associates maintain a business associate agreement.

II. Requirements. All business associate agreements shall include, at a minimum, the following clauses:

A. A description of the uses and disclosures of PHI that are permitted and required by the services agreement and the business associate agreement.

1. The business associate agreement may not authorize the business associate to use or further disclose the information in a manner that would violate HIPAA if done by Chimes, except that:

    i. The business associate agreement may permit the business associate to use and disclose PHI for its own proper management and administration, including:

        a. Uses for the proper management and administration of the business associate;

b. Uses to carry out the legal responsibilities of the business associate;

c. Disclosures required by law;

d. Disclosures where the business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

ii. The business associate agreement may permit the business associate to provide data aggregation services relating to the health care operations of Chimes.

B. Provisions that address the following:

1. No further uses or disclosures other than as permitted or required by the contract or required by law;

2. The use of appropriate safeguards to prevent the use or disclosure of PHI other than as provided by the contract;

3. The reporting of any uses or disclosures not provided for by the contract of which the business associate is aware;

4. Ensure that any agents or subcontractors of the business associate agree to the same terms and conditions that the business associate has agreed to in its business associate agreement with Chimes with respect to PHI;

5. Ensure that any agents or subcontractors are able to provide each of the individual rights under HIPAA and carry out those rights on behalf of Chimes to the extent applicable;

6. A requirement that the business associate will, to the extent it is to carry out Chimes' obligations under 45 CFR Subpart E, if any, comply with those requirements of 45 CFR Subpart E that apply to Chimes in the performance of such obligations;

7. Make all internal practices, books, and records relating to the uses and disclosures of PHI available to the Secretary of the Department of Health and Human Services;

8. At the end of the contract return or destroy all PHI; however, if return or destruction is determined not to be feasible, the protections of the business

associate agreement shall continue for as long as the business associate retains the PHI;

9. A term and termination clause, including a termination clause which specifies the effect of termination and any reference to a later survival clause or section;

10. A provision making the business associate a Qualified Service Organization if Substance Use Disorder Information will be disclosed; and

11. Language including 42 CFR Part 2 requirements.

C. A clause permitting the termination of the contract if the business associate violates a material term of the business associate agreement. If termination is not feasible, the problem must be reported to the Secretary of Department of Health and Human Services.

D. HIPAA Security Rule requirements, including:

1. A requirement that the business associate implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic PHI (ePHI);

2. A requirement that the business associate ensure that any agents or subcontractors agree to implement reasonable and appropriate safeguards to protect ePHI; and

3. A requirement that security incidents are reported to Chimes.

E. Specific clauses with regard to how the business associate shall meet the requirements of the Breach Notification Rule found at 45 CFR §§ 164.400-164.414.

F. A requirement that the business associate report to Chimes any security incident of which it becomes aware, including breaches of unsecured protected health information as required by 45 CFR § 164.410.

G. The Privacy Official will also consider the following clauses or sections as a part of the business associate agreement:

1. An indemnification clause;

2. A requirement for the business associate to carry insurance regarding any privacy or security breaches;

3. A statement indicating that there are no third-party rights created as a part of the business associate agreement;

4. Consideration of agency and fiduciary issues between the parties;

5. Consideration of any issues associated with the Genetic Information and Non Discrimination Act of 2008 (GINA);

6. A requirement that the business associate encrypt all electronic devices in compliance with the April 2009 (or any subsequent) HHS Guidance regarding the technologies and methodologies that render PHI unusable, unreadable or indecipherable;

7. Prohibitions or restriction on the PHI being permitted to be transmitted to any offshore vendors;

8. A survival clause regarding the protections and extension of other non-required clauses (such as indemnification and insurance);

9. Any state law concerns or considerations;

10. Common legal considerations including survival, interpretation and conflict of clauses, notice requirements, and documentation that this is the entire agreement regarding this subject and that the business associate agreement supersedes any prior writings or understandings;

11. If the Business Associate may perform any marketing services or will be marketing, that company will abide by state laws; and

12. A section requiring the business associate to use standard transactions and code sets as required by 45 CFR § 162.923(c) when conducting any Standard Transactions on behalf Chimes.

III. Substance Use Disorder Information

A. Chimes shall only disclose Substance Use Disorder Information to a Qualified Service Organization. Any business associate or other third party who receives substance use disorder information must be Qualified Service Organization, and any information disclosed must be limited to the information needed by the Qualified Service Organization to provide services to Chimes.

1. A Qualified Service Organization is any individual or entity who:

   i. Provides services to Chimes (such as data processing, bill collecting, dosage preparation, laboratory analyses, or legal, accounting, population health management, medical staffing, or other professional services, or services to prevent or treat child abuse or neglect, including training on nutrition and childcare and individual and group therapy), and

   ii. Has entered into a written agreement with Chimes that:

a. Acknowledges that in receiving, storing, processing, or otherwise dealing with any patient records from Chimes, it is fully bound by the regulations at 42 CFR Part 2; and

b. If necessary, will resist in judicial proceedings any efforts to obtain access to patient identifying information related to substance use disorder diagnosis, treatment, or referral for treatment except as permitted by 42 CFR Part 2.

B. The Privacy Official shall ensure that any business associate agreement with a Qualified Service Organization includes provisions that the Qualified Service Organization:

1. Acknowledges that in receiving, storing, processing, or otherwise dealing with any patient records from Chimes, it is fully bound by the regulations at 42 CFR Part 2; and

2. If necessary, will resist in judicial proceedings any efforts to obtain access to patient identifying information related to substance use disorder diagnosis, treatment, or referral for treatment except as permitted by 42 CFR Part 2.

C. Disclosures of Substance Use Disorder Information shall be limited to the information needed by the Qualified Service Organization to provide services.

IV. Monitoring Compliance. If Chimes discovers or suspects that a business associate/qualified service organization is inappropriately using or disclosing or failing to protect PHI, the Privacy Official will investigate the concern immediately. If the concern is determined to be valid, the Privacy Official shall notify the business associate/qualified service organization of the concern immediately and take appropriate follow-up given the level of concern.

V. Termination. At the termination of any business associate relationship, the Privacy Official, in consultation with the Security Official, will determine whether it is feasible for the business associate to return or destroy all Chimes PHI maintained by that business associate. If the Privacy Official determines that return or destruction is not feasible, the Privacy Official will document this determination and document that such PHI is still maintained by the business associate. The Privacy Official will also remind the business associate, in writing, of its obligation to continue to protect PHI in accordance with the terms of the business associate agreement for as long as the business associate retains such PHI.

VI. Record Retention. The Privacy Official shall maintain all business associate agreements for no less than six (6) years from termination or six (6) years from the date when all PHI in possession of the business associate has been destroyed and a certification of such destruction has been obtained by Chimes.

REGULATORY REFERENCES

42 CFR § 2.11
45 CFR § 164.308
45 CFR § 164.314
45 CFR § 164.504(e)

Chimes Privacy Policies & Procedures	
Title: Program Document Retention	**No. P024**
Responsible Party: Privacy Official Security Official	Implementation Date: April 10, 2019
Last Reviewed Date: December 5, 2025	Revision History: 4/10/19; 10/1/19; 5/1/23, 1/15/26

POLICY

Chimes retains copies of all policies and procedures and all communications that are required to be in writing by HIPAA and this Program. Chimes also retains records of actions or designations that HIPAA requires to be documented.

Materials can be maintained in written or electronic form and must be maintained for six (6) years from the date of creation or when they were last in effect, whichever is later.

All workforce members are expected to comply with this Policy. Any person who fails to abide by the rules of the Policy may be subject to disciplinary action, up to and including termination of employment or contract.

PROCEDURES

I. General Procedures

A. Chimes identifies records and documents by their category. The Privacy Official or his or her designee identifies records and documents as either containing or not containing PHI to ensure proper retention and storage.

B. To the extent that a document or record falls into more than one document category, the document or record should be retained under the category with the longer retention timeframe.

C. Chimes will document and retain all necessary policies for compliance with federal and state laws regarding information privacy and security and will make all policies and procedures available to its employees who deal with PHI or other sensitive information in their work.

1. Chimes retains copies of its policies and procedures as well as all communications that are required to be in writing. Chimes also retains records of actions or designations that HIPAA requires to be documented. HIPAA requires certain documents to be maintained for at least six (6) years from the date of creation or when they were last in effect, whichever is later. A document checklist of examples of documents that must be kept under this procedure is found in the Record Retention Schedule. Please note, documents in this category may also fall into another document category requiring a longer retention period.

2. The Privacy Official is responsible for

i. Retaining all requests for individual rights including access, restrictions, amendments and accounting of disclosures and the responses to such requests;

ii. Collecting and storing documentation/logs for audit purposes (disclosures for purposes other than treatment, payment, health care operations, or in response to written authorizations);

iii. Documenting all circumstances where a customer has requested and received an accounting of disclosures of PHI;

iv. Maintaining a file of business associate agreements and related agreements;

v. Maintaining a file of privacy and other related complaints received and corrective actions taken.

3. Human Resources is responsible for:

i. Maintaining documentation of training regarding privacy and security;

ii. Documenting which personnel have received such training; and

iii. Maintain documentation of sanctions applied to workforce members for any violations of HIPAA or the policies and procedures maintained as a part of this Program.

4. The Privacy Official and the Security Official will keep documentation of the classifications of personnel and their level of access to PHI.

D. All records that are either sent to storage or archived will be clearly labeled by document category and filed with a destruction date designated. Situations in which storage or archived files are not marked for destruction or where documents are retained beyond the indicated destruction date will be brought to the attention of the Security or Privacy Official.

E. The Privacy Official will ensure that a valid HIPAA Business Associate Agreement is in place with all vendors that provide storage or record destruction services for records containing PHI.

II. Legal Holds

A. In the event any staff member is made aware of either active litigation or a potential claim involving Chimes, that staff member shall notify the Security Official.

B. The Security Official shall evaluate the claim, with assistance from the executive team and outside legal counsel, and shall determine whether it should order the immediate cessation of the destruction schedule for all relevant documents.

C. When a legal hold is necessary, legal counsel will immediately inform management and/or the Security Official. Legal counsel will outline the matter and provide specific examples of the types of information to be retained, including applicable date ranges

D. The Security Official or Privacy Official will coordinate the legal hold process by:

1. Identifying possible sources of data, including email;

2. Identifying custodians of applicable documents and email and informing those individuals of their duty to retain documents and/or emails; and

3. Taking all steps necessary to ensure that essential documents and/or emails are retained.

E.

REGULATORY REFERENCES

45 CFR § 164.312(c)
45 CFR § 164.316(b)
45 CFR § 164.530(j)

Record Management Schedule

HIPAA RECORDS	PERIOD OF RETENTION
Examples that may be retained as part of the clinical record include: • Requests, responses and records related to any individual rights requests, including requests for access, amendment, restrictions or accounting of disclosures. • Logs of disclosures for accounting purposes. • Authorizations to release records, responses to authorizations to records requests. • Personal Representative Forms. • Information in Designated Record Sets to which patients have access. • Court orders, grand jury subpoenas, etc., where disclosure is required by law. • Written statements in connection with disclosures needed for other judicial/administrative processes, where the disclosure is not mandated by court order. • Notices terminating a restriction on uses or disclosures of PHI previously agreed to. • Written statements by agencies or officials supporting suspension of an accounting of PHI Disclosures (including documented oral statements). Examples of other types of HIPAA-related documentation: • All HIPAA compliance policies and procedures, including any revisions. • Business Associate Agreements, Data Use Agreements and any related agreements. • Notices of Privacy Practices. • Complaints about compliance with HIPAA, HIPAA-related policies and procedures, and the disposition of those complaints. • Documentation of sanctions applied to employees for violations of HIPAA or the Program. • Group health plan amendments and certifications, including any revisions. • Conclusions and supporting analysis from an expert that health information is de-identified.	6 years from the date of creation or when they were last in effect, whichever is later