jssa

JSSA
HIPAA
POLICIES AND PROCEDURES

THE INA KAY BUILDING, 200 WOOD HILL ROAD, ROCKVILLE, MD 20850 | 240-800-JSSA | JSSA.org

HIPAA POLICIES AND PROCEDURES

The Jewish Social Service Agency ("JSSA") recognizes that client information is sensitive and must be treated carefully and responsibly. JSSA therefore has implemented these "HIPAA Policies and Procedures" to guide JSSA's use and disclosure of protected health information ("PHI") in accordance with the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as expanded and amended by the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH"), along with their implementing regulations. The HIPAA Policies and Procedures outline JSSA's Compliance Program for complying with HIPAA, including the Privacy Rule, Security Rule, and Breach Notification Rule, and relevant state laws.

Each JSSA workforce member (staff, volunteers, consultants, and vendors) is expected to follow the HIPAA Policies and Procedures and to otherwise assist in maintaining the confidentiality of client information. Compliance with these HIPAA Policies and Procedures means that workforce members may not be permitted to have access to healthcare and billing records or that workforce members may have access to only certain sections of these records. Compliance with these HIPAA Policies and Procedures also means that in some instances special paperwork may need to be completed or that client/patient information may not be used or disclosed in certain ways.

JSSA workforce members must review JSSA's HIPAA Policies and Procedures carefully and make sure that they understand them. All workforce members should contact JSSA's Privacy Officer regarding any questions about how to manage a situation involving the use or disclosure of PHI, including clients' medical or billing information to as "JSSA" in these policies and procedures.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

TABLE OF CONTENTS

Oversight of HIPAA Policies and Procedures 7
General Overview 8
Maintaining the Confidentiality of Protected Health Information 8
Filing of Complaints, Reporting Potential Violations, and Protection of Individual Rights 8
Responding to Complaints and Potential Violations 8
Policies and Procedures and Required Documentation 9
HIPAA Training 10
Sanctions for Non-Compliance with HIPAA Policies and Procedures 11
Investigation of Potential Breaches 11
Internal Sanctions 11
Professional Sanctions 12
Criminal and Civil Sanctions 12
Documentation 12
Release of Protected Health Information 13
I. General Information 14
II. Verification 15
III. Minimum Necessary Rule 16
IV. Treatment, Payment, and Healthcare Operations 16
V. Involvement in Care and Notification Purposes 16
VI. Public Policy Uses and Disclosures 17
VII. Fundraising and Marketing 17
VIII. Sale of Protected Health Information 18
IX. Authorizations 18
X. Valid Authorizations 18
XI. Revoking Authorizations 19
XII. Documenting Authorizations 19
Personal Representatives 20
Determination of Status as Personal Representative 20
Decisions to Not Treat a Person as a Personal Representative 20
Content of Notice of Privacy Practices 21
Distribution of Notice of Privacy Practices 21
Acknowledgement of Receipt of Notice of Privacy Practices 21
Restrictions on Types, Means, and Locations of Uses and Disclosures of Protected Health Information 22
I. Right to Request Restriction of Uses and Disclosures 22
II. Right to Request Confidential Communications 22
Access by Patients to Protected Health Information 23
I. General Policy Regarding Access by Patients/Clients to their PHI 23
II. Requests for Access 23
III. Granting of Access 23
IV. Denial of Access 24
Amendment of Protected Health Information 25
I. General Healthcare Record Modification Policy 25

©2026 JSSA. All rights reserved. Proprietary to JSSA.

II. Requests for Amendment 25
III. Granting of Requests 25
IV. Denial of Requests 26
V. Correction and Amendment Procedure 27
Accounting of Disclosures of Protected Health Information 28
I. General Policy Regarding Accountings of Disclosures of PHI 28
II. Requests for Accounting of Disclosures 28
III. Granting of Accountings of Disclosures 29
Business Associates 30
Determination of Business Associate Status 30
Execution of Business Associate Agreement & Required Terms 30
Response to Violation of Business Associate's HIPAA Obligations 30
Overall Communication: General Guidelines 32
Verbal Communication 32
Mobile Phone 32
Texting 32
Email 32
Written Communication 32
Fax 33
Social Media 33
Internet Video 33
Photographs and Video 33
Other 33
Email Policy 34
Emails Containing Confidential Information 34
Guidelines: Emails Sent to a JSSA Email Address AND to an External Email Address 34
Transmission of Confidential Information 35
Transmission of Appointment Reminder Emails 35
Printing Email Messages 35
Retention Policy 36
Fax Policy 37
Breach of Unsecured Protected Health Information 38
I. Definitions 38
II. Investigations Following Breach or Potential Breach 39
III. Required Notifications 40
IV. Business Associates 41
V. Training and Sanctions 41
Security Management Process 42
Risk Analysis & Risk Management 42
Information System Activity Review 42
Access Authorization 43
I. Granting Access 43
II. Modifying Access 44
III. Terminating Access 44
IV. Responsibilities 44
V. Documentation 45

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Information System Security 46
Method for Accessing JSSA's Information System 46
Security Training & Reminders 46
Prevention of Unauthorized Access to JSSA's Information System 46
Protection from Malicious Software 47
Log-In Monitoring 47
Password Management 47
Security Incident Procedures 48
Response and Reporting of Security Incident Procedures 48
Contingency Plan 49
Preparation for Emergencies 49
I. Data Backup 49
II. Protection of JSSA Network 49
III. Revision of Emergency Response Plan 49
IV. Emergency Response 50
Facility Access Controls 51
Physical Access Authorization, Modification, and Termination 51
Physical Access to JSSA Facilities 51
Physical Access to Locations Within JSSA Facilities 52
Workstation Set-up and Use 53
Workstation Locations 53
Workstation Area Set-up 53
Workstation Use – Protection of JSSA Information Network and PHI 53
Workstation Use – General Use Guidelines 54
Internet Security 55
Portable Computer and Mobile Device Use 56
Portable Computers 56
Mobile Phones and other Mobile Devices 57
Off-Site Work 58
Maintaining Confidentiality of PHI 58
Security of PHI 58
Device and Media Controls 59
Device and Media Tracking 59
Destruction of PHI 59
Media Re-Use 60
Encryption and Decryption 61
Encryption Policy 61
Encryption Standard 61
Exception to Encryption Requirement 61
Information Integrity 62
Data Integrity 62
Appendix A: Additional Resources 63
Appendix B: HIPAA Policy and Procedure Definitions 64
JSSA 64
Workforce Member 64
Business Associate 64

©2026 JSSA. All rights reserved. Proprietary to JSSA.

PHI 64
Direct Service Provider 64
Appendix C: Appointment Reminder Template 65
Appendix D: Version Control 66

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Oversight of HIPAA Policies and Procedures

JSSA has appointed a Privacy Officer who is responsible for the development, implementation, and oversight of JSSA's HIPAA Policies and Procedures, including the development, implementation, maintenance, and revision of all HIPAA Policies and Procedures related to compliance with the HIPAA Privacy, Security, and Breach Notification Rules. The current Privacy Officer is JSSA's Director of Compliance and Continuous Quality Improvement.

To assist the Privacy Officer in carrying out these responsibilities, JSSA also has appointed a Healthcare Information Security Officer ("HISO") who is responsible for assisting the Privacy Officer ("PO") with the protection of PHI. The current HISO is JSSA's Chief Information Officer ("CIO"). The PO and HISO may designate additional staff to assist with implementation.

The PO is responsible for:

- Overseeing the development, implementation, and operation of JSSA's HIPAA Policies and Procedures;
- Providing leadership on HIPAA matters to any privacy board, committee, or task forces created by JSSA;
- Developing and implementing JSSA's training program for compliance with the HIPAA Policies and Procedures;
- Monitoring the effectiveness of the HIPAA Policies and Procedures;
- Workforce security training and awareness;
- Initiating and overseeing the completion of corrective action plans for violations of the HIPAA Policies and Procedures;
- Developing and maintaining a copy of JSSA's Notice of Privacy Practices and ensuring acknowledgements, authorizations, and other forms are on file;
- Receiving and responding to complaints about how JSSA uses and discloses PHI and to questions regarding matters covered in JSSA's Notice of Privacy Practices;
- Developing, implementing, and overseeing JSSA's procedures for addressing accommodation requests and requests for access, amendments, and accountings; and
- Monitoring developments under the Administrative Simplification provisions of HIPAA and periodically revising the HIPAA Policies and Procedures as necessary.

The HISO is responsible for:

- Management of system technology to support information privacy and security requirements;
- Maintenance of confidentiality, integrity, and availability of data as the privacy and security programs integrate;
- Development and maintenance of security policies and procedures including management of security risk assessments, the program budget, security complaints and incident activity, and enforcement;
- Monitoring the effectiveness of the HIPAA Policies and Procedures;
- Workforce security training and awareness;
- Application of industry standards and best practices;
- External compliance assurances and security survey activity; and
- Business continuity planning.

The HISO also serves as the security voice on the Safety and Security Committee for decision-making around information security decisions for internal and health information exchange business decisions.
JSSA workforce members should address any questions concerning the scope, use, or disclosure of PHI to the PO. All JSSA workforce members are responsible for complying with the requirements of JSSA's HIPAA Policies and Procedures.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

General Overview

Maintaining the Confidentiality of Protected Health Information

JSSA will maintain the confidentiality of PHI and other sensitive information. PHI will be used or disclosed only as permitted or required by HIPAA, HIPAA's implementing regulations, other applicable state and federal law, and these HIPAA Policies and Procedures.

JSSA will train its workforce members on HIPAA requirements. JSSA workforce members are responsible for complying with the requirements of JSSA's HIPAA Policies and Procedures and reporting any potential violations to the PO. Any workforce member who does not comply with these requirements is subject to disciplinary action, up to and including termination.

Filing of Complaints, Reporting Potential Violations, and Protection of Individual Rights

Any individual, including workforce members, patients, and patients' family members, may raise issues or register complaints regarding any of JSSA's HIPAA Policies and Procedures concerning the use and disclosure of PHI and/or JSSA's compliance with these HIPAA Policies and Procedures. Complaints and grievances should be submitted to the PO or the Secretary of the U.S. Department of Health and Human Services (the "Secretary"), as described in JSSA's Notice of Privacy Practices.

JSSA will not require individuals to waive their rights to file a complaint with the Secretary or their other rights under HIPAA as a condition to receiving treatment. JSSA will not retaliate against any person, patient, or JSSA workforce member who files a complaint with the Secretary or PO or testifies, assists, or participates in investigations, compliance reviews, proceedings, or hearings under the Administrative Simplification provisions of HIPAA.

All workforce members are prohibited from intimidating, threatening, coercing, discriminating against, or otherwise retaliating against a client/patient for exercising any right granted under HIPAA or participating in any process established by HIPAA or its implementing regulations, such as the filing of a complaint against JSSA. Any JSSA workforce member found to have retaliated against any individual (including patients and other workforce members) in violation of these HIPAA Policies and Procedures will be subject to disciplinary action, up to and including termination.

Responding to Complaints and Potential Violations

The PO or designee will be responsible for overseeing or conducting an investigation into all complaints and reports of potential HIPAA violations and taking corrective measures, as necessary. The PO or designee will report the outcome of investigations to JSSA's executive management as warranted. The PO or designee will document and maintain a copy of all complaints and reports received and the dispositions of such complaints and reports. This documentation will be maintained by the PO or designee for at least six (6) years from the date of its creation or when it was last in effect, whichever is later.

JSSA will take all reasonable steps necessary to mitigate any harmful effect of the inappropriate use or disclosure of PHI whenever it becomes aware of any violation of HIPAA Policies and Procedures. This requirement applies whether the harm is created by JSSA or one of its business associates.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Policies and Procedures and Required Documentation

JSSA has reasonably designed its HIPAA Policies and Procedures to comply with the standards, implementation specifications, and other requirements of HIPAA and its implementing regulations, taking into account JSSA's size and the type of activities undertaken by JSSA. A copy of the HIPAA Policies and Procedures and all related policies will be posted on JSSA's shared drive and will be available from the PO.
JSSA will modify its HIPAA Policies and Procedures as necessary to comply with changes in state and federal law, including changes to the HIPAA regulations, or to reflect changes in JSSA's operations (e.g., growth, change to electronic healthcare records). These changes will be documented and implemented promptly. If a change in law materially affects the content of JSSA's Notice of Privacy Practices, the PO will make the appropriate changes to the Notice of Privacy Practices in a timely manner. All HIPAA Policies and Procedures will be documented and contain a version number and effective date. This documentation will be maintained by the PO for at least six (6) years from the date the applicable version of the HIPAA Policies and Procedures was created or was last in effect, whichever is later.

JSSA will maintain the original or a copy of communications required to be in writing and documentation of actions, activities, designations, or assessments that must be documented under the HIPAA regulations and as specified by these HIPAA Policies and Procedures. This documentation will be maintained by the PO and HISO for at least six (6) years from the date of its creation or when it was last in effect, whichever is later. Necessary documentation will be available to those persons responsible for implementing the procedures to which the documentation pertains.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

HIPAA Training

JSSA will provide training on JSSA's HIPAA Policies and Procedures for all workforce members with access to personally identifiable health information and protected health information. All new workforce members will complete required training within 30 calendar days of hire. JSSA will provide a minimum of one (1) hour per year of refresher training to workforce members, which will include training on significant changes in JSSA's HIPAA Policies and Procedures. If there is a significant change to the HIPAA Policies and Procedures based on law or practice, JSSA will retrain those workforce members that access information covered under HIPAA. Supplemental training will be provided as necessary or as requested.

HIPAA training for all workforce members with access to personally identifiable health information will include, but is not limited to, the following subjects:

- Principles of and need for privacy and security;
- Requirements of HIPAA and HITECH regulations;
- JSSA's HIPAA Policies and Procedures regarding health information;
- Guidance for protecting data integrity and confidentiality, such as proper password/log-in procedures for computer workforce members, how to guard against computer viruses, securing documents with individually identifiable health information, and the like;
- Procedures for reporting breaches of security and confidentiality, and
- Ramifications of breaches of security and confidentiality.
- Confidentiality requirements applicable to substance use disorder–related information under 42 CFR Part 2, including permitted uses, disclosures, and redisclosure restrictions.

JSSA workforce members must sign an attestation and acknowledgement when they have completed all HIPAA-related training, including initial and refresher training. The Director of Human Resources is responsible for managing the training documentation to include records of completion ("Training Records"). These Training Records will be retained for at least six (6) years from the date of training.

Please see the Statement of Acknowledgment and Agreement for additional information.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Sanctions for Non-Compliance with HIPAA Policies and Procedures

As a condition of employment or other affiliation with JSSA, all JSSA workforce members are required to follow JSSA's HIPAA Policies and Procedures. JSSA will impose appropriate disciplinary action, in accordance with JSSA's progressive discipline procedures.

A copy of JSSA's progressive discipline process can be found in JSSA's Employee Handbook or is available by contacting the Director of Human Resources.

Investigation of Potential Breaches

Any workforce member of JSSA who believes that another workforce member, agent, or contractor of JSSA has breached JSSA's HIPAA Policies and Procedures or otherwise breached the integrity or confidentiality of client/patient or other sensitive information should immediately report such breach to the PO.

The PO or designee will conduct a thorough and confidential investigation into the allegations. JSSA will not retaliate, discriminate, or permit reprisals against a complainant or workforce member who participates in an investigation. Allegations not made in good faith will be sanctioned in accordance with JSSA's progressive discipline procedures.

Internal Sanctions

Senior management and department heads/supervisors are responsible for disciplining workforce members in an appropriate and consistent manner. The type of disciplinary action shall be determined on a case-by-case basis, and, where appropriate, in consultation with the PO, the Chief Human Resources Officer, and/or other appropriate members of management, if any.

JSSA's progressive disciplinary procedures, described in detail in JSSA's Employee Handbook, sanctions generally become more severe for repeated infractions. JSSA's progressive disciplinary procedures, however, do not mandate the use of a lesser sanction before JSSA terminates a workforce member. At the discretion of the Chief Human Resources Officer and senior management, as appropriate, JSSA may terminate a workforce member for the first breach of JSSA's HIPAA Policies and Procedures if the seriousness of the offense warrants such action.

- A workforce member should expect to lose his or her job for a willful or grossly negligent breach of confidentiality, willful or grossly negligent destruction of computer equipment or data, or knowing or grossly negligent violation of HIPAA, its implementing regulations, any other federal or state law protecting the integrity and confidentiality of client/patient information, or JSSA's HIPAA Policies and Procedures. Termination also may be appropriate if a workforce member commits any act, such as selling client/patient names or records, which would expose JSSA to potential criminal sanctions; fails to report conduct that the workforce member knew was a violation of JSSA's HIPAA Policies and Procedures, HIPAA, its implementing regulations, or any other applicable federal or state law; or fails to correct behavior for which the workforce member was previously disciplined.
- A workforce member may lose his or her job for a negligent breach of JSSA's standards for protecting the integrity and confidentiality of client/patient information. For less serious breaches, management may impose a lesser sanction, such as a verbal or written warning, verbal or written reprimand, loss of access, suspension without pay, demotion, requirement. to take additional training or other sanction.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

JSSA will seek to include violations by contractors as a ground for termination of the contract and/or imposition of contract penalties.
Failure to cooperate in an investigation or inquiry conducted by the PO may subject the non-cooperative individual to the disciplinary policy and sanctions discussed above.

Professional Sanctions

Violations of JSSA's HIPAA Policies and Procedures or standards may violate professional ethics and be grounds for professional discipline. Any individual subject to professional ethics guidelines and/or professional discipline should expect JSSA to report such violations to appropriate licensure/accreditation agencies and to cooperate with any professional investigation or disciplinary proceedings.

Criminal and Civil Sanctions

Violation of JSSA's HIPAA Policies and Procedures or standards may constitute a civil or criminal offense under HIPAA or other federal and/or state laws. Any workforce member or contractor who violates a civil or criminal law may expect that JSSA will provide information concerning the violation to appropriate law enforcement personnel or regulatory agency, and JSSA will cooperate with any law enforcement investigation or prosecution.

Documentation

Documentation of any sanctions applied for any actions covered by JSSA's HIPAA Policies and Procedures will be maintained by Human Resources for at least six (6) years from the date that the sanction is applied.

The HIPAA Policies and Procedures are intended to serve as a guide for the efficient and professional performance of duties of JSSA's workforce members to protect the integrity and confidentiality of healthcare and other sensitive information. Nothing herein shall be construed to be a contract between the employer and the workforce member. Additionally, nothing in the HIPAA Policies and Procedures is to be construed by any employee as containing binding terms and conditions of employment. Nothing in the Policies should be construed as conferring any employment rights on employees or changing their status from "at-will employees." JSSA retains the absolute right to terminate any workforce member, at any time, with or without good cause. Management retains the right to change the contents of the Policies as it deems necessary with or without notice.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Release of Protected Health Information

JSSA has a legal and an ethical responsibility to preserve the privacy and confidentiality of client/patient Protected Health Information ("PHI"). JSSA will use and disclose PHI only as permitted by HIPAA and these HIPAA Policies and Procedures. PHI refers to individually identifiable health information transmitted or maintained in any format (written, electronic, or oral), whether related to a living or a deceased individual.

Certain records maintained by JSSA may include substance use disorder (SUD)–related information subject to additional federal confidentiality protections under 42 CFR Part 2. When PHI includes SUD-related information, JSSA will comply with both HIPAA and applicable Part 2 requirements. Where Part 2 imposes more stringent protections or conditions than HIPAA, JSSA will follow Part 2.

JSSA may use and disclose PHI in the following situations:

- To the individual;
- For treatment, payment, and health care operations;
- For facility directories and certain notification purposes such as disaster situations, so long as the individual has an opportunity to agree or object;
- For public policy purposes specified by the HIPAA regulations;
- For fundraising purposes (with written authorization);
- For remunerated treatment communications that are not considered marketing activities;
- Pursuant to a valid authorization;
- Incident to an otherwise permitted or required use or disclosure.

JSSA also will disclose PHI in the following circumstances:

- To an individual pursuant to a request for access or for an accounting of disclosures.
    - Requests for access will be responded to in accordance with JSSA's Access by Clients/Patients to PHI Policy.
    - Requests for accountings of disclosures will be responded to in accordance with JSSA's Accountings of Disclosures of PHI Policy.
- When required by the Secretary.
    - All requests from the Secretary immediately will be sent to the PO. The PO or designee is responsible for responding to any such requests.

JSSA will abide by the following provisions when using or disclosing PHI:

- JSSA will not use or disclose PHI in violation of a request for a restriction to which it has agreed.
    - Requests for restrictions will be handled in accordance with JSSA's Restrictions on Types, Means, and Locations of Uses and Disclosures of PHI Policy.
- JSSA will use or disclose PHI in accordance with reasonable requests by an individual to receive communications of PHI by alternative means or at alternative locations.
    - Requests for communication by alternative means or at alternative locations will be handled in accordance with JSSA's Restrictions on Types, Means, and Locations of Uses and Disclosures of PHI Policy.

Before making any permitted disclosure, JSSA will take reasonable steps to verify the identity of the person requesting PHI, the authority of the person to access the requested PHI, and that any required documentation, statements, or representations have been obtained and meet the necessary requirements.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

When using, disclosing, or requesting PHI, JSSA will make reasonable efforts not to use, disclose, or request more than the minimum amount of PHI necessary to accomplish the intended purpose of a use, disclosure, or request.

If health information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual, then the health information is not PHI and may be used or disclosed. The PO or designee must confirm that health information is or has been de-identified appropriately before the health information may be used or disclosed.

I. General Information

- JSSA will process requests for information from client/patient records in a timely, consistent manner and only with written and signed authorization if appropriate and required. Information may be released either in hard copy form, electronic form, or verbally.

  Hard copies and/or electronic copies of any portion of the client/patient record may be released only by designated workforce members as defined by the PO.

  Information may be released verbally only by designated workforce members including but not limited to the following:
  - Patient Accounts Staff
  - Quality Improvement Coordinator
  - Direct Service Providers
  - Compliance Specialist/Assistant
  - Chief Executive Officer ("CEO"), COO, PO

- These HIPAA Policies and Procedures apply equally to electronic records, such as email, fax, internet or other electronically maintained or transmitted PHI. No workforce members will release electronic records without complying with these HIPAA Policies and Procedures.

- If appropriate, JSSA will prepare a cover letter for hard copy releases detailing the items included in a use or disclosure. Unless a law or regulation requires a more specific prohibition on re-disclosure, each disclosure outside JSSA will contain the following notice:

  "The attached healthcare information pertaining to above named individual is confidential and legally privileged. JSSA has provided it to you as authorized by the client/patient or as otherwise authorized by HIPAA. The recipient may not further disclose the information without the express consent of the client/patient or as authorized by law."

- Designated JSSA workforce members will maintain a log to track the step-by-step process toward completion of each request for release of information. Designated JSSA workforce members will review and update this log regularly to give proper priority to requests and to provide early intervention in problem situations.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

- JSSA will retain the original request, the authorization (if applicable), and a copy of the cover letter in the client/patient's record for the appropriate record retention period for healthcare and business-related records and/or in accordance with JSSA's Records Retention and Destruction Policy.

II. Verification

- Prior to any disclosure, JSSA workforce member must:
    - Verify the identity of a person requesting PHI and the authority of such person to have access to PHI (except for uses or disclosures requiring the opportunity for an individual to agree or object);
        - For example, if the requester states that the requester is from law enforcement, request to see a badge or credentials. If the requester states that the requester is from the Department of Health to audit healthcare records, ask to see documentation of the authorization on Department letterhead. Unless something about the badge, credential, letter on Department letterhead or other proof of authority appears suspicious, the workforce member can rely on such evidence.
    - Obtain any documentation, statements, or representations from the person requesting the PHI when they are a condition of the disclosure.

- JSSA may rely, if reasonable, on any of the following to verify an individual's identity when the disclosure is to a public official or a person acting on behalf of the public official:
    - If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;
    - If the request is in writing, the request is on the appropriate government letterhead;
    - If the disclosure is to a person acting on behalf of a public official, 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.

- JSSA may rely, if reasonable, on any of the following to verify an individual's authority to access PHI when the disclosure is to a public official or a person acting on behalf of the public official:
    - 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; or
    - If a request is made pursuant to legal process, a warrant, subpoena, order, or other legal process issued by a grand jury, or a judicial or administrative tribunal is presumed to constitute legal authority.

  See the Government Request for Information, Investigations, Search Warrants and Subpoenas Policy for additional information.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

III. Minimum Necessary Rule

- JSSA will not use, disclose or request more than the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure, or request.
- The minimum necessary rule does not apply to:
    - Disclosures to/requests by a health care provider for treatment.
    - Uses or disclosures made to an individual, including pursuant to an individual's request for access to PHI or for an accounting of disclosures.
    - Uses or disclosures made pursuant to an authorization.
    - Disclosures to the Secretary to enforce compliance.
    - Uses or disclosures required by law.
    - Uses or disclosures required for compliance with HIPAA.

- When the minimum necessary rule applies, JSSA may not use, disclose, or request an entire healthcare record, except when the entire healthcare record is justified.

- Department Directors must enforce the implementation of this policy.

- JSSA will analyze each request to ensure that only the minimum necessary information is released.

- JSSA may rely, if reasonable under the circumstances, on a requested disclosure as the minimum necessary when:
    - Making disclosures to public officials, if the public official represents that the information is the minimum necessary for the stated purpose(s);
    - The information is requested by another covered entity;
    - The information is requested by a professional who is a member of its workforce or is a business associate of JSSA for the purpose of providing professional services to JSSA, if the professional represents that the information is the minimum necessary for the stated purpose(s).

IV. Treatment, Payment, and Healthcare Operations

- JSSA may disclose PHI in connection with treatment, payment, or health care operations without written authorization. This includes JSSA's own treatment, payment, or health care operations as well as the treatment or payment activities of another health care provider.

- A written authorization is required for uses or disclosures of PHI for marketing, the sale of PHI, and fundraising purposes (except for those described below).

- When treatment, payment, or health care operations involve SUD-related information subject to 42 CFR Part 2, JSSA workforce members must ensure that disclosures are permitted under Part 2 and consistent with the scope of any applicable patient consent or authorization.

V. Involvement in Care and Notification Purposes

- With verbal authorization, JSSA may verbally disclose to a family member, other relative, a close personal friend, or any other person identified by the client/patient, PHI relevant to such person's involvement with the client/patient's care or payment related to care.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

- With written authorization, JSSA may disclose to a family member, other relative, a close personal friend, or any other person identified by the client/patient, documentation (in any format) containing PHI relevant to such person's involvement with the client/patient's care or payment related to care.

- JSSA may disclose the client/patient's location, general condition, or death (including disclosing information to a public or private entity assisting with disaster relief efforts) to notify, or assist in the notification of a family member, a personal representative, or another person responsible for the care of the client/patient. When feasible, JSSA will only provide this information under special circumstances and after consultation with and approval of the Privacy Officer.

- If the patient/client is deceased, JSSA may disclose PHI to a family member, other relative, a close personal friend, or any other person identified by the individual who was involved in the individual's care or payment for healthcare prior to the patient/client's death to the extent that the PHI is relevant to the person's involvement. JSSA will not disclose PHI for this purpose if doing so is inconsistent with a prior expressed preference of the patient/client known by JSSA.

VI. Public Policy Uses and Disclosures

- Generally, JSSA may use or disclose PHI without a written authorization or opportunity for the client/patient to agree or object for certain specified public policy purpose. Requests for uses or disclosures of PHI for public policy purposes should be sent immediately to the PO.

- JSSA workforce members will respond to government search warrants, subpoenas, and document requests by referring them to JSSA's PO. Please see JSSA's Government Request for Information, Investigations, Search Warrants, and Subpoenas Policy for additional information.

VII. Fundraising and Marketing

- JSSA may use demographic information relating to an individual, dates of health care provided to an individual, treating physician name, outcome information, and health insurance status for the purpose of raising funds for its own benefit. JSSA also may disclose this information to a business associate or to an institutionally related foundation for these purposes.

- JSSA will include a statement in its Notice of Privacy Practices stating that JSSA may use PHI for fundraising purposes. JSSA may not use the PHI for fundraising purposes if this statement is not included in the Notice of Privacy Practices.

- JSSA fundraising activities that involve the use or disclosure of PHI will comply with the following restrictions:
    - Each fundraising communication made to an individual will provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for electing not to receive further communications must not cause the individual to incur an undue burden or more than a nominal cost.
    - Treatment or payment will not be conditioned on the individual's choice with respect to the receipt of fundraising communications.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

- No fundraising communications will be made to an individual who has elected not to receive further communications.
- JSSA may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications.

- A valid authorization is required for any use of PHI for fundraising or marketing purposes.

VIII. Sale of Protected Health Information

JSSA does not sell PHI.

IX. Authorizations

- JSSA may not use or disclose PHI without a valid authorization, except as otherwise set forth in this policy and permitted by HIPAA. The use or disclosure must be consistent with the authorization.

- JSSA generally must obtain an authorization for any use or disclosure of psychotherapy notes. Authorizations for the use or disclosure of psychotherapy notes may not be combined with authorizations for other uses and disclosures. An authorization is not required for:
  - Use by the originator of the psychotherapy notes for treatment;
  - Use or disclosure by JSSA for its own training programs;
  - Use or disclosure by JSSA to defend itself in a legal action or other proceeding brought by the individual; or
  - Use or disclosure required by law, permitted by HIPAA for health oversight activities with respect to the oversight of the originator of the psychotherapy notes, to coroners and medical examiners, or to prevent a serious and imminent threat to the health or safety of the individual or public.

- JSSA generally must obtain an authorization for any use or disclosure of PHI for marketing.

X. Valid Authorizations

- JSSA will use the approved authorization form unless required to use a form from governmental agencies or other sources. JSSA will use the required form from a governmental agency or other source only if the non JSSA form includes all of the required elements included in the JSSA approved authorization form.

- A valid authorization must be written in plain language and contain the following:
  - A specific and meaningful description of the information to be used or disclosed.
  - Specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.
  - Specific identification of the person(s), or class of persons, to whom JSSA may make the requested use or disclosure.
  - A description of each purpose of the requested use or disclosure.
  - A date range of the information that is to be used or disclosed.
  - An expiration date or an expiration event.
  - The signature of the individual and 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.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

- Statements that inform the individual of the following information:
  - The client or other authorized person may revoke the authorization at any time, except to the extent that action has been taken in reliance upon it, by providing written notice to JSSA's PO.
  - JSSA may not condition treatment, payment, enrollment, or eligibility for benefits on whether the individual signs the authorization.
  - Information disclosed pursuant to the authorization may be subject to restrictions on further use or re-disclosure under applicable federal and/or state confidentiality laws, including HIPAA and 42 CFR Part 2.

- If JSSA seeks an authorization from an individual for a use or disclosure of PHI, JSSA must provide the individual with a copy of the signed authorization.

- Any concerns or questions regarding the validity of an authorization should be referred to the PO for review.

XI. Revoking Authorizations

- An individual may revoke an authorization in writing at any time, except to the extent that JSSA has taken action in reliance thereon. The revocation will become effective no sooner than the date on which JSSA receives it.

- Revocations must be given to the Privacy Officer.

XII. Documenting Authorizations

- JSSA must document and retain in the client/patient's record any signed authorization **for a period of no less than six (6) years from the date on the authorization.**

- Authorizations that are not valid will not be retained in the client/patient's record and will be saved by the Privacy Officer or designee in a secure system.

Please see JSSA's Authorization to Release Information form, Client Request for Information form, Designation of Authorized Representative and Release of Information form, Liability and Publicity Release form, and Media Filming Authorization form for additional information.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Personal Representatives

JSSA generally will treat a verified personal representative of a client/patient as the client/patient for the purposes of these HIPAA Policies and Procedures. Verification includes receipt of legal documentation from the representative confirming their designation as a personal representative.

If a JSSA workforce member is unsure if a person qualifies as the personal representative of a client/patient or is otherwise permitted to be provided with PHI related to the client/patient, the JSSA workforce member will inform the PO immediately. The PO is responsible for determining whether the person is a personal representative of the client/patient and/or is otherwise permitted to be provided with PHI. No PHI will be disclosed to the person until the PO has made the required determination.

Determination of Status as Personal Representative

Client/Patient Category	Personal Representative
Adult Emancipated Minor	A person with legal authority to make health care decisions on behalf of the individual. *Examples:* Health care power of attorney Court appointed legal guardian General power of attorney
Unemancipated Minor	A parent, guardian, or other person acting *in loco parentis* with legal authority to make health care decisions on behalf of the minor child. *Exceptions:* See below
Deceased	A person with legal authority to act on behalf of the decedent or the estate (not restricted to health care decisions) *Examples:* Executor of the estate Administrator of the estate Next of kin (surrogate) or other family member
For additional information, see U.S. Department of Health and Human Services, Office of Civil Rights December 3, 2002, Guidance Explaining Significant Aspects of the HIPAA Privacy Rule.	

Decisions to Not Treat a Person as a Personal Representative

Abuse, Neglect, and Endangerment Situations

JSSA may choose to not treat a person as the personal representative of a person if:

- JSSA has a reasonable belief that:
    - 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
- JSSA decides that it is not in the best interest of the individual to treat the person as the individual's personal representative in the exercise of professional judgment.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Content of Notice of Privacy Practices

The PO is responsible for developing and maintaining the Notice of Privacy Practices required by the HIPAA Privacy Rule. A copy of JSSA's Notice of Privacy Practices will be retained for at least six (6) years from the date it was last in effect.

JSSA will use and disclose PHI only in a manner consistent with its Notice. The PO will amend the Notice of Privacy Practices and/or these HIPAA Policies and Procedures as necessary to ensure that the Notice of Privacy Practices and these HIPAA Policies and Procedures are consistent with each other; JSSA's actual practices regarding the use and disclosure of PHI; HIPAA and the HIPAA implementing regulations; and state law. To the extent that JSSA engages in any activities that can only be performed when they are included in the Notice of Privacy Practices (e.g., sale of PHI, fundraising), the PO will be responsible for ensuring that the Notice of Privacy Practices includes the required statements.

As part of the Notice of Privacy Practices, JSSA will reserve the right to make any revised Notice of Privacy Practices effective for PHI received or maintained prior to the date the revised Notice of Privacy Practices becomes effective. The Notice of Privacy Practices will be revised promptly whenever there is a material change to JSSA's practices described in the Notice. Unless required by law, material revisions will not be implemented prior to the effective date of the revised Notice.

The PO will be listed on the Notice and serve as the contact person for individuals who have complaints about how JSSA has used or disclosed their PHI or who have questions about JSSA's Notice.

Please see JSSA's current Notice of Privacy Practices for additional information.

Distribution of Notice of Privacy Practices

A copy of the Notice shall be distributed to each client/patient before any services are provided. A copy of the Notice (and/or revised Notice) will be prominently displayed in a public location that is easily visible to all workforce members, clients/patients, and visitors. JSSA also will post the Notice in a prominent location on its web site and make the Notice available electronically through the web site. The PO or designee will provide additional copies of the Notice to individuals, including members of the public, in electronic or paper format upon request.

Acknowledgement of Receipt of Notice of Privacy Practices

Prior to initiation of service, the primary service provider is responsible for ensuring that the Notice is distributed properly and for obtaining clients/patients' acknowledgment and signature that they received a copy of the Notice. This signed acknowledgement is retained in the client/patient record.

JSSA will maintain documentation of the client/patient's written acknowledgment of receipt of the Notice for at least six (6) years from the date the documentation was created or was last in effect, whichever is later.

Please see JSSA's current Notice of Privacy Practices for additional information.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Restrictions on Types, Means, and Locations of Uses and Disclosures of Protected Health Information

All Requests for written documentation containing PHI MUST Go to The Privacy Officer or Designee

I. Right to Request Restriction of Uses and Disclosures

- JSSA will give consideration to requests to restrict certain uses and disclosures of PHI on a case-by-case basis. All requests for restrictions must be made in writing.

- The PO or designee is responsible for approving or denying all such requests.

- JSSA must grant requests to restrict disclosures of PHI about the individual to a health plan if (1) the disclosure is for the purpose of carrying out payment or health care operations, (2) the disclosure is not otherwise required by law, and (3) the PHI pertains solely to a health care item or service for which the individual, or a person on behalf of the individual (other than the health plan) has paid JSSA in full.

- If JSSA agrees to a request for restriction, JSSA may not use or disclose PHI in violation of such restriction, except for emergency treatment.
    - If a disclosure is made to another provider in an emergency situation, JSSA will request that the provider not further use or disclose the information.
    - A restriction agreed to by JSSA is not effective to prevent disclosures to the Secretary of HHS or uses or disclosures for public policy purposes.

- JSSA may terminate its agreement to a restriction, if:
    - The individual agrees to or requests the termination in writing;
    - The individual orally agrees to the termination and the oral agreement is documented; or
    - JSSA informs the individual that it is terminating its agreement, except that the termination is only effective with respect to PHI created or received after the individual was informed.
        - JSSA may not terminate requests to restrict disclosures of PHI to a health plan that it is required to grant.

- JSSA will file a copy of the request for restriction (and/or termination) and the PO's decision regarding whether to grant (and/or terminate) the restriction in the client/patient's healthcare record and billing record.

II. Right to Request Confidential Communications

- JSSA will permit client/patient to request that JSSA provide confidential communications of PHI to the individual by alternative means or at alternative locations. Communication preferences must be documented in the Client Consent and Acknowledgements form. Verbal requests for a change in communication preferences must be documented or the request must be in writing and retained in the client/patient record.

- JSSA will accommodate all reasonable requests to receive communications by alternative means or at alternative locations.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Access by Patients to Protected Health Information

I. General Policy Regarding Access by Patients/Clients to their PHI

JSSA will comply with an individual's right to access their PHI or record. Such requests should be forwarded to the Privacy Officer or designee for prompt processing. A client/patient generally has a right of access to inspect and obtain a copy of PHI in their designated record set, for as long as the PHI is maintained.

This right to access does not apply to:

- Psychotherapy notes;
- Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

II. Requests for Access

- All requests for client/patient access to PHI contained in a designated record set must be in writing.

- The PO or assigned designee is responsible for receiving and processing requests for access by individuals and retaining all required documentation, as specified by these HIPAA Policies and Procedures.
    - All requests received for access to PHI must be logged and processed.
    - Consultation with licensed clinical staff regarding the request for access will be made, if necessary.

- JSSA must act on a request no later than 30 days after receipt or otherwise specified by state law. If JSSA is unable to take an action in the required time, JSSA may extend the time once by no more than 30 days, provided that, within the required time limit, JSSA provides a written statement of the reasons for the delay and the date by which JSSA will complete its action on the request.

- JSSA must document and retain the designated record sets that are subject to access by client/patient.

III. Granting of Access

- JSSA will provide a client/patient with access to their PHI unless grounds for a denial exist.

- If JSSA provides a client/patient with access, in whole or in part, JSSA must:
    - Provide the access in form/format (including an electronic form/format if the PHI is maintained electronically) requested, if readily producible; if not, in a readable hard copy form or such other form/format agreed to by JSSA and the client/patient. In certain circumstances, JSSA can provide a written summary instead.
    - Provide the access in a timely manner as applicable by stated and federal regulations. JSSA may discuss the scope, format, and other aspects of the request with the individual to facilitate timely access.

- JSSA may charge a reasonable fee to cover certain of its costs (as specified by the HIPAA regulations) related to providing a copy or summary of the PHI to the individual in response to the request for access. JSSA may waive fees for good cause. JSSA will not charge more than the maximum fee permitted under state law, regardless of the actual costs incurred in responding to a request for access.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

IV. Denial of Access

- JSSA may deny access without an opportunity for review for:
    - PHI to which the right of access does not apply.
    - PHI pertaining to an individual JSSA is treating on behalf of a correctional institution.
    - Certain research purposes.
    - PHI subject to the Privacy Act, 5 U.S.C. 552a.
    - PHI obtained from someone other than JSSA under a promise of confidentiality if access would likely reveal the source of the information, such as personnel records held by government agencies.

- All JSSA clients have the right to review their healthcare record. However, JSSA may deny access when:
    - A licensed health care professional, in the exercise of professional judgment, determines access is likely to endanger the life or physical safety of the individual or another person;
    - The PHI makes reference to another person (other than a health care provider) and a licensed health care professional, in the exercise of professional judgment, determines the access is likely to cause substantial harm to such other person; or
    - The request for access is made by the individual's personal representative and a licensed health care professional, in the exercise of professional judgment, determines that access by such personal representative is likely to cause substantial harm to the individual or another person.

- If JSSA denies access, in whole or in part, JSSA must:
    - To the extent possible, give the individual access to any other PHI requested, after excluding the PHI for which JSSA has a ground to deny access.
    - Provide a timely, written denial to the individual.
    - If JSSA does not maintain the requested PHI but knows where it is maintained, inform the individual where to direct the request for access.

- If access is denied, the individual has the right to request review of the denial. JSSA promptly will designate a licensed health care professional who was not directly involved in the denial to review the decision. The designated individual must determine, within a reasonable period of time, whether or not to deny the requested access. JSSA must provide or deny access in accordance with the designated individual's determination. JSSA must promptly provide written notice to the client/patient of the designated individual's decision and take other action as required to carry out the reviewing official's determination.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Amendment of Protected Health Information

JSSA will comply with an individual's rights to request amendment to their PHI or record. Such requests should be processed promptly, especially in cases in which failure to correct the information could result in a negative client/patient outcome.

I. General Healthcare Record Modification Policy

- JSSA may modify a client/patient record as the result of a client/patient request. If a Direct Service Provider believes that a modification of the record is required, JSSA will modify a client/patient record under the following circumstances:
    - Incorrect client/patient information has been entered into the client/patient record;
    - Client/patient information has been entered into an incorrect client/patient record; or
    - A form has been duplicated or an incorrect form was created containing PHI.

II. Requests for Amendment

- All requests for amendment of information contained in a client/patient record must be in writing. The request will provide a reason for the request and will specify the amendment requested. A written description of JSSA's policy on requests for amendment shall be provided to all clients/patients in JSSA's Notice of Privacy Practices.

- Designated staff are responsible for receiving and processing requests for amendments by individuals and retaining all required documentation, as specified in these HIPAA Policies and Procedures.
    - Requests received for amendment are logged and processed.
    - Requests for amendment will be brought to the attention of the appropriate direct service staff and/or supervisor.

- In coordination with the PO and only with the PO's approval, designated workforce members may grant or deny client/patient requests to amend their PHI or records.

- All requests must be acted upon no later than 60 days after receipt of the request. If JSSA is unable to act on the request within the 60-day period, JSSA may extend the time by no more than 30 days, provided that JSSA notifies the client/patient in writing prior to the expiration of the 60-day period of the reasons for the delay and the date by which JSSA will respond to the request. By law, JSSA is entitled to only one 30-day extension.

III. Granting of Requests

- If the decision is made to amend the record as requested by the client/patient, the client/patient will be notified in writing within 10 business days of the decision. JSSA will request from the client/patient a list of relevant persons/entities who should receive a copy of the amendment and authorizations from the client/patient to forward the amendment to the persons/entities so identified by the client/patient.

- The direct service provider (clinician, nurse, case manager, etc.) must notify the designated workforce member, in writing, of any persons/entities, including business associates, believed, or known to have health information that is the subject of the amendment and that relied, or could foreseeably rely, on such

©2026 JSSA. All rights reserved. Proprietary to JSSA.

information to the detriment of the individual. JSSA must make reasonable efforts to inform and provide the amendment to these persons/entities. The designated workforce member is responsible for ensuring that all such persons/entities are promptly notified of the amendment.

- If JSSA is informed by another covered entity of an amendment to an individual's PHI, JSSA must amend the PHI in the client/patient record as provided in this Policy.

IV. Denial of Requests

- JSSA may deny a client/patient amendment request if JSSA determines that the information sought to be amended meets any of the following criteria:
    - The current information is accurate and complete.
    - The current information was not created by JSSA, unless the individual making the request can provide to JSSA a reasonable basis to believe that the originator of the information is no longer available to act on the request.
    - The information is not part of the patient's designated record set.
    - The information is not available to the client/patient for inspection.

- JSSA will do the following when a request is denied:
    - Provide a written statement to the individual making the request within 60 days or 90 days during an extension.
    - The written statement of denial:
        - Uses plain language.
        - Explains the basis for the denial.
        - States that the individual is entitled to provide a written statement disagreeing with JSSA's denial and provide instructions on how to file the statement of disagreement.
        - States that if the individual does not submit a statement of disagreement, the individual may request that JSSA provide the individual's request for amendment and JSSA's denial with any subsequent disclosure of the PHI that is the subject of the request.
        - Provides a description of how the individual can complain to JSSA pursuant to JSSA's Grievance Policy including the name, title, and telephone number of the designated JSSA contact person for the receipt of complaints, or to the Secretary of HHS pursuant to HIPAA requirements.

- JSSA will permit the client/patient to submit a written statement of disagreement with the denial. JSSA may reasonably limit the length of the written statement of disagreement.

- JSSA may issue a written rebuttal to the client/patient's written statement of disagreement. If a rebuttal is issued, JSSA shall provide a copy to the client/patient.

- Designated staff must identify the record or PHI in the client/patient record that is the subject of the disputed amendment and append or otherwise link the client/patient's request for amendment, JSSA's denial of the request, the client/patient's written statement of disagreement, if any, and JSSA's rebuttal, if any, to the client/patient record.
    - If a statement of disagreement has been submitted by the client/patient, JSSA must include the material above, or, at the election of JSSA, an accurate summary of any such information, with any subsequent disclosure of the PHI to which the disagreement relates.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

- If the client/patient has not submitted a written statement of disagreement, JSSA 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.
- When a subsequent disclosure is made using a standard transaction that does not permit the additional material to be included with the disclosure, JSSA may separately transmit the required material, as applicable, to the recipient of the standard transaction.

V. Correction and Amendment Procedure

- Mental Health Services - Depending on location, the workforce member will notify the Clinical Director if a health care record needs modification.

- Hospice – Workforce member must notify the Program Director or Clinical Supervisor if a healthcare record needs modification.

- Homecare – Workforce member must notify the Program Director if a healthcare record needs modification.

- The workforce member will provide the name of the record, the form in the record that needs modification and the explanation for what and why the record needs to be changed.

- Designated staff will make the modification and amendment and log the modification and amendment in the Quality Assurance Record Modification Log.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Accounting of Disclosures of Protected Health Information

I. General Policy Regarding Accountings of Disclosures of PHI

JSSA will comply with an individual's right to receive an accounting of disclosures of their PHI made by JSSA in the six (6) years prior to the date on which the request for the accounting was made.

- JSSA must document and retain:
  - The information required to be included in an accounting; and
  - The written accounting that is provided to the client/patient.

- Generally, an accounting must include:
  - Disclosures made during the six (6) years (or shorter time period, as requested) prior to the date of the request, including disclosures to or by business associates of JSSA.
  - The date of the disclosure.
  - The name of the entity or person who received the PHI and, if known, their address.
  - A brief description of the PHI disclosed.
  - A brief statement of the purpose of the disclosure or, in certain circumstances, a copy of a written request for a disclosure.

- Disclosures that do not need to be included in an accounting include the following:
  - Disclosures for treatment, payment, and health care operations;
  - Disclosures to individuals of their own PHI;
  - Disclosures incident to a valid use or disclosure;
  - Disclosures pursuant to an authorization;
  - Disclosures to persons involved in the individuals care, or for other permitted notification purposes;
  - Disclosures for national security or intelligence purposes;
  - Disclosures to correctional institutions or law enforcement officials

- All workforce members must inform the PO immediately of any requests from a health oversight agency or law enforcement official to temporarily suspend an accounting of disclosures to an individual.

II. Requests for Accounting of Disclosures

- All requests for accounting of disclosures of client/patient PHI must be in writing.

- The PO is responsible for receiving and processing requests for accountings of disclosures and retaining all required documentation, as specified in this policy.

- JSSA must act on a request no later than 60 days after receipt. If it cannot, JSSA may extend the time once by no more than 30 days, provided that within 60 days JSSA provides a written statement of the reasons for the delay and the date by which JSSA will provide the accounting.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

III. Granting of Accountings of Disclosures

- JSSA will provide the first accounting in any 12-month period without charge.
- JSSA may charge a reasonable, cost-based fee for each subsequent request by the same individual within the 12-month period. JSSA will inform the requesting individual of the fee in advance and provide the individual with an opportunity to withdraw or modify the request for the accounting in order to avoid or reduce the fee. JSSA may waive fees for good cause.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Business Associates

The PO is responsible for ensuring that PHI is not shared with a business associate before a written business associate agreement has been executed.

Determination of Business Associate Status

Before sharing information with a third-party service provider, including an agent, subcontractor, or other party with whom JSSA conducts business, the PO will determine whether PHI is going to be shared with or accessible by the third-party service provider and if the third-party service provider will be a business associate, as defined by HIPAA.

Execution of Business Associate Agreement & Required Terms

JSSA will not disclose PHI to a business associate unless JSSA has first received satisfactory assurances that the business associate will appropriately safeguard the PHI and has executed a Business Associated Agreement ("BAA") with the business associate which contains all of the provisions required by law. The PO is responsible for securing the appropriate BAA from all of JSSA's business associates.

Where a business associate creates, receives, maintains, or transmits SUD-related information subject to 42 CFR Part 2, the business associate agreement must require compliance with applicable Part 2 confidentiality and redisclosure requirements.

JSSA will ensure that all of its BAA's require the business associate to promptly notify JSSA after discovery of a breach of unsecured PHI, as defined in the Breach of Unsecured PHI Policy, so that JSSA can provide the notifications required by the Breach Notification Rule within sixty (60) calendar days of when the business associate first knew or should have known about the breach. Each business associate agreement will require the business associate to provide JSSA with any and all information JSSA requires to comply with its notification requirements, including the identification of each individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during a breach.

A copy of JSSA's standard BAA template is available in JSSA's shared drive.

Response to Violation of Business Associate's HIPAA Obligations

If JSSA becomes aware of a pattern of activity or practice of a business associate that constitutes a material breach or violation of the business associate's obligations under its contract, JSSA will take reasonable steps to cure the breach or end the violation. Steps that JSSA may take include the following:

- requiring the business associate to submit periodic reports to JSSA concerning its privacy, security, and breach notification practices;
- requiring the business associate to reacquire, at its expense, any information it inappropriately sold to a third party; or
- requiring, as a condition of keeping its contract with JSSA, that the business associate terminate the employee (or end the relevant arrangement with the workforce member) of the business associate responsible for the breach.

If the business associate violation cannot be corrected or cured, JSSA will terminate the agreement, where feasible. The PO will have the authority to terminate a business associate contract, subject to the approval of

©2026 JSSA. All rights reserved. Proprietary to JSSA.

the Chief Executive Officer of Chief Operating Officer. Where there are no feasible alternatives to the business associate, JSSA may choose not to terminate.

Please see JSSA's Business Associate Agreement Policy for additional information.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Overall Communication: General Guidelines

All communications involving PHI, including phone, email, fax, texting, social media, or other means of communication, must be made in accordance with the Overall Communication: General Guidelines Policy.

Verbal Communication

Workforce members should follow these rules regarding client PHI:

- Do not discuss client information in public areas including hallways and stairwells, restaurants, coffee shops (Starbucks), etc. Do not discuss client information at conferences, symposiums, seminars, and other types of public gatherings.
- Do not raise your voice to communicate client information in or across offices. Be mindful that your voice or the voice of your client may carry to other offices, hallways, etc.
- Do not discuss client information with JSSA staff not authorized to receive client information.
- Staff must be mindful of verbal communications with clients to ensure privacy of client information.
- Do not assume that speaking with a client or other staff person in another language protects the client or JSSA from violating HIPAA. HIPAA applies to all languages including American Sign Language.
- If you recognize a client outside of JSSA, maintain professional boundaries. Do not initiate a conversation with that client.
- If a client recognizes you and initiates a conversation with you, maintain professional boundaries and do NOT identify yourself as a JSSA workforce member. You are permitted to acknowledge the client speaking to you but limit your conversation as much as possible.

Mobile Phone

- Please refer to appropriate conduct under JSSA's Mobile Phone Policy.

Texting

- Workforce members are not permitted to communicate with clients and/or collateral contacts regarding client information via text message. This includes texting on personal and JSSA provided equipment. Exceptions may be made but only with the expressed permission of the PO.
- Texting clients and/or collateral clients automatically discloses your mobile phone number. Workforce members are not permitted to disclose their mobile number to clients.

Email

- Please refer to JSSA's Email Policy for appropriate use.

Written Communication

- All requests for any written correspondence (letters to schools, parents, doctors, etc.) and/ or for the release of full or partial healthcare records must be reviewed and approved in advance by the PO or designated staff.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

- Before any written communication, ensure you have a current and valid authorization to release information. This requirement applies to requests coming directly from the client. Clients must sign JSSA's Authorization for Release of Information form.
- When communicating in writing, only provide the minimum amount of information necessary. Do not provide additional information that has not been requested.

Fax

- Please refer to JSSA's Fax Policy for appropriate use of JSSA fax machines.

Social Media

- Please refer to JSSA's Social Media Policy for appropriate/permitted behavior in using social media in your position at JSSA.

Internet Video

- The use of internet communications technologies, including Skype, Facetime, and other audio/video technologies is allowed following applicable laws and regulations.
- Use of these technologies must be approved in advance by the PO and/or the HISO.

Photographs and Video

- Photographs and video recording of JSSA clients/patients are not permitted unless they are for business purposes only. This restriction applies to the use of cell phone cameras or other types of cameras.
- Photographs or videos of clients are permitted if the photograph is taken using the client/patient's camera at their request.

Other

- The use of Google, Yahoo, Bing or other search engine tools or any social media outlets to research, obtain information or otherwise look up a client is strictly prohibited. This activity violates the client's privacy.
- Exceptions may be made on a case-by-case basis and only with the approval of the program director or the PO.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Email Policy

- The email system and all messages generated by or managed by email, including back-up copies, are part of the business equipment of JSSA, are owned by JSSA, and are not the property of workforce members.
- Consequently, workforce members *do not have a right to privacy in their use of the computer system or its email component*.
- JSSA reserves the right to monitor, audit, delete, and read email messages to support operational, maintenance, auditing, security, and investigative activities.
- Generally, workforce members should restrict their use of the email system to proper business purposes relating to the care and treatment of clients/patients and related administrative matters, such as billing. A workforce member may, however, use email for personal purposes, such as communicating a change in work schedule to a significant other, under the following conditions:
    - Personal use does not involve significant use of the facility's resources, such as work time, computer time, costs, and the like, and does not preempt any business activity or interfere with the workforce member's or other's productivity.
    - When using email for personal purposes, staff must use their personal email account system (Gmail, Yahoo, Hotmail, Verizon, Comcast, etc.) and not their jssa.org email.
    - Workforce member must not transmit confidential or proprietary information to unauthorized recipients. Proprietary information is information that belongs to JSSA.
    - Workforce member must not transmit obscene, offensive, harassing, or hostile messages to any recipient. No person shall enter, transmit, or maintain messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual orientation, or health condition. No person shall enter, maintain, or transmit any abusive, profane, or offensive language.
    - Transmission must not involve any illegal or unethical activity.
- The email system will employ usernames and associated passwords to isolate the communications of different workforce members.
- Workforce members must never share passwords or reveal them to anyone else.
- Because some information is intended for specific individuals and may not be appropriate for general distribution, workforce members should exercise caution when replying, forwarding, and copying (CC & BCC) messages.
- Professional judgment should be used to discern whether an email message sent or received concerning the diagnosis or treatment of a client/patient should become a part of that client/patient's record.
- Workforce members are not permitted to share their personal email addresses with clients and/or collateral contacts including, but not limited to, client's family, school social worker or guidance counselor.
- Clients/patients must consent to the use of email for the secure transmission of confidential health information per JSSA's Client Rights and Responsibilities Policy.
- Clients/patients must consent to the use of email for the purpose of appointment reminders.
- Workforce members must immediately report violations of this policy to their department heads and to the PO.

Emails Containing Confidential Information

Guidelines: Emails Sent to a JSSA Email Address AND to an External Email Address

- Workforce member should adhere to minimum necessary rule when communicating about business or treatment matters. That is, keep the amount of information communicated to the absolute minimum based on the situation.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

- Workforce member should acknowledge receipt of message.
- Client Information
    - Whenever possible, use client initials only.
    - Do not include unrelated or extraneous information in the message.
    - No detailed information about the client. Communicate client details via phone.
- Email Address
    - Sender is responsible for verifying that the email address is correct before sending.
    - If confidential information is sent to an incorrect address, you are required to immediately report the matter to the PO.
- No client/patient name or other confidential information can be included in the subject line of the message.

Transmission of Confidential Information

- Workforce members must adhere to the minimum necessary rule. That is, keep the amount of information communicated to the absolute minimum based on the situation.
- Any email sent to the client, family member, a personal representative, or another person responsible for the care of the client/patient must be sent secure ("encrypted").
- Any email sent from a non-JSSA address (such as a volunteer) to a JSSA address containing confidential information must use JSSA's Secure Email service.
- JSSA volunteers who have a JSSA email account must use their JSSA email account.
- To ensure a recipient is aware that you will be sending them a secure message, workforce member should alert the recipient in advance.
- For messages sent internally (within JSSA's email system), you do NOT have to send a secure ("encrypted") email.

Transmission of Appointment Reminder Emails

- Clients/patients must consent to the use of email for the purpose of appointment reminders. Consent is included in JSSA's Client Rights and Responsibilities Policy.
- If consent is given, appointment reminder emails can be sent using regular, unsecure email.
- Appointment reminder emails may only be sent using an authorized template. You may change the date and/or time but no other changes are permitted.
- Whenever you send an appointment reminder or discuss an appointment, create a new email message using the template. Do not reply directly to the client's email. Directly replying may inadvertently include protected health information.

Printing Email Messages

- Workforce member must use their professional judgment when determining which emails should be printed and placed in the client/patient record.
- In general, emails that contain service-related information should be uploaded into the client's record.
    - These types of email should be printed as a pdf and uploaded into the client's record.
    - You must not copy and paste email messages into a progress note.
- Printed email messages that are not part of the client/patient record must be shredded using an approved JSSA shredder.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Retention Policy

- See JSSA Records Retention and Destruction Policy for the retention and deletion of email messages.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Fax Policy

All workforce members must strictly observe the following standards relating to facsimile communications of client/patient healthcare records:

- Healthcare records or documents containing individually identifiable health information may be transmitted by fax only when urgently needed for client/patient care or required by a third-party payer for payment.
- Information transmitted must be limited to that necessary to meet the requester's needs.
- A cover page must accompany all fax transmissions containing individually identifiable health information and include the confidentiality notice, except in cases where instructed not to, such as Medicare Appeals.
- Reasonable efforts must be made to assure that the fax transmission is sent to the correct destination. For a new recipient, the sender must verify the fax number before sending the fax and verify the recipient's authority to receive confidential information.
- Designated administrative support staff is responsible for ensuring that incoming faxes are properly managed—not left sitting on or near the machine or in email, but rather are distributed to the proper recipient expeditiously while protecting confidentiality during distribution such as by sealing the fax in an envelope.
- Any misdirected faxes or violations of this Fax Policy must be reported immediately in accordance with the Breach of Unsecured Protected Health Information Policy.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Breach of Unsecured Protected Health Information

JSSA is committed to protecting our client/patients' privacy and confidentiality. As part of this commitment, JSSA maintains the confidentiality of PHI in accordance with applicable law and regulations and JSSA's HIPAA policies and procedures. JSSA shall notify individuals, the Secretary, and the media of certain breaches of unsecured PHI in accordance with this HIPAA Policy.

I. Definitions

- Unsecured PHI: PHI that is not secured through the use of a technology or methodology identified by the Secretary to render the PHI unusable, unreadable, and undecipherable to unauthorized persons. Unsecured PHI may be written, oral or electronic information.

  Unsecured PHI does not include the following information:
  - De-identified health information, which, by definition, is not PHI.
  - PHI which has been encrypted according to an encryption algorithm for which the confidential decryption key or process has not been breached. The encryption key must be kept on a separate device or at a separate location from the encrypted data to ensure that the key is not breached.
  - PHI which has been destroyed, i.e., there has been destruction of the media on which the PHI is stored or received so that either (1) paper, film, or other hard copy have been shredded such that PHI cannot be read or reconstructed, or (2) electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitation such that PHI cannot be retrieved.

  Redaction does not satisfy the requirements for destruction, but redaction may be used to de-identify the health information so that the information is no longer considered PHI.

  Unsecured PHI may include information contained in Limited Data Sets.

- Breach: the acquisition, access, use or disclosure of PHI in a manner not permitted under HIPAA which compromises the security or privacy of the PHI. Breach does not include:
  - Unintentional acquisition, access, or use of PHI by a member of JSSA's workforce or an individual acting under JSSA's authority or under the authority of a business associate, provided such unintentional activity was done in good faith, within the course of employment or other professional relationship, and does not result in further use or disclosure that is not permitted by HIPAA.
  - Inadvertent disclosure of PHI by a person with authority to access PHI at JSSA or business associate to another person who also has authority to access PHI at JSSA or the same business associate, provided the recipient does not further use or disclose the information in a manner not permitted by HIPAA.
  - Unauthorized disclosures of PHI where, based on the good faith belief of the disclosing person, the recipient to whom the PHI is disclosed would not reasonably have been able to retain the information.

- A breach is discovered on the first day on which the breach is known or should have been known by the exercise of reasonable diligence, by any person, other than the person committing the breach, including any workforce member, agent, or business associate of JSSA.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

- A breach is known when the incident is first known, or should have been known by exercising reasonable diligence, even if it is not initially clear whether the incident constitutes a breach.

II. Investigations Following Breach or Potential Breach

- All workforce members and agents will report to the PO if the workforce member or agent knows or has reason to believe that a breach has occurred. Failure to report knowledge of a breach or potential breach will be grounds for disciplinary action, up to and including termination.

- Following the discovery of a breach or potential breach, JSSA will begin an investigation and conduct a risk assessment to determine whether a breach actually has occurred. If a breach of Unsecured PHI occurred, JSSA will determine the notifications that must be made as a result of the breach in accordance with this Policy.

- The PO or designee will act as the investigator of the breach or potential breach. The investigator will be responsible for the management of the breach investigation, completion of the risk assessment, and coordinating with others in JSSA as appropriate (e.g., administration, security incident response team, human resources, risk management, public relations, legal counsel, etc.). The investigator will oversee the process of sending any notifications required as a result of the breach.

- All documentation related to the breach investigation, including the risk assessment and proof that all notifications were made as required, will be retained for a minimum of six years. JSSA will maintain documentation sufficient to meet its burden of proof with respect to demonstrating that all notifications were made or that the use or disclosure of PHI did not constitute a breach of Unsecured PHI.

- The risk assessment and supporting documentation must be fact specific and address:
    - Whether the disclosure was impermissible under HIPAA; and
    - Whether there is a low probability that the unauthorized activity compromises the security or privacy of the PHI based on a risk assessment of at least the following factors:
        - The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
        - The identity of the unauthorized person who used the PHI or to whom the disclosure was made;
        - Whether the PHI actually was acquired or viewed; and
        - The extent to which the risk to the PHI has been mitigated.
    - (JSSA will presume that an unauthorized acquisition, access, use, or disclosure of PHI is a breach unless it determines that there is a low probability that the security or privacy of the PHI has been compromised based on this risk assessment.)

- JSSA will maintain a written log of all breaches of Unsecured PHI, in addition to the reports created for each incident. The PO or designee will be responsible for maintaining this log. The information contained in this log will be used to create the annual report submitted to the Secretary of HHS described below. For each incident, the log will include, to the extent possible:
    - A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of individuals affected, if known;

©2026 JSSA. All rights reserved. Proprietary to JSSA.

- A description of the types of Unsecured PHI involved in the breach (such as full name, Social Security number, date of birth, home address, account number, diagnosis, etc.);
- A description of the action taken with regard to notification of clients/patients regarding the breach; and
- Steps taken to mitigate the breach and prevent future occurrences.

III. Required Notifications

- Following the discovery of a breach of Unsecured PHI, JSSA will provide notice to client/patient, as described below, without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach or potential breach.

- JSSA will, following the discovery of a breach of Unsecured PHI, notify each individual whose Unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of such breach.

- JSSA will notify an individual in writing by first class mail or by e-mail (if the individual has agreed to receive information by e-mail) of any breaches of Unsecured PHI. If JSSA knows the individual is deceased and has the address of the individual's next of kin or personal representative, JSSA will send the required notification by first class mail to the next of kin or personal representative.

- If the individual's contact information is insufficient or out-of-date, a substitute form of notice reasonably calculated to reach the individual will be provided. Substitute notice is not required when there is insufficient or out-of-date contact information that precludes notification to the next of kin or personal representative of the individual.

- If the breach involves fewer than 10 individuals with insufficient or out-of-date contact information, JSSA will provide substitute notice by an alternative form of written notice, e- mail, telephone, or other means. If the breach involves 10 or more individuals with insufficient or out-of-date contact information, JSSA will place a conspicuous notice on JSSA's website home page for 90 days or in a major print or broadcast media in the area where the affected individuals likely reside. The notice will include a toll-free phone number that will remain active for 90 days where an individual can learn whether the individual's Unsecured PHI may be included in the breach.

- If JSSA determines that notifications must be made with urgency because of possible imminent misuse of Unsecured PHI, an alternative form of notification, such as by telephone, may be used in addition to the required written notification.

- If a breach involves more than 500 individuals in a state or jurisdiction, JSSA will send notices to prominent media outlets serving the state or jurisdiction. Notification will be made without unreasonable delay and in no event later than 60 calendar days. This notification is in addition to the notification provided directly to the individuals. Notification of media outlets is not required if no single state or jurisdiction has more than 500 affected individuals.

- If a breach involves 500 or more individuals, regardless of whether no single state or jurisdiction has more than 500 affected individuals, JSSA will notify the Secretary of HHS contemporaneously with notification to the individuals. Notice will be provided to the Secretary in the manner specified on the HHS website.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

- JSSA will submit an annual report to the Secretary of HHS not later than 60 days after the end of each calendar year documenting all breaches discovered during the preceding year involving fewer than 500 individuals. JSSA will submit the report in the manner specified on the HHS website.

- JSSA will delay notifications if a law enforcement official tells JSSA that a notification, notice or posting would impede a criminal investigation or cause damage to national security. If the statement is in writing and specifies the time for which a delay is required, JSSA will delay the notification for the time period specified by the official. If the statement is made orally, JSSA will document the statement, including the identity of the official making the statement, and delay notification temporarily, but not for more than 30 days from the date of the oral statement, unless a written statement is submitted to JSSA during that time.

- The notices required under this HIPAA Policy will be written in plain language and include the following:
    - A brief description of the breach, including the date of the breach and the date of its discovery, if known;
    - A description of the types of Unsecured PHI involved in the breach;
    - Steps the individual should take to protect himself/herself from potential harm resulting from the breach;
    - A brief description of the actions JSSA is taking to investigate the breach, mitigate harm to the individual, and protect against further breaches; and
    - Contact information, including a toll-free telephone number, e-mail address, website, or postal address, to permit the individual to ask questions or obtain additional information.

IV. Business Associates

- JSSA will ensure that all its BAA's require that the business associate notify JSSA promptly and in no case later than 30 calendar days after discovery of a breach of Unsecured PHI.

- The BAA's will require the business associate to provide JSSA with any and all information JSSA requires to comply with its notification requirements.

V. Training and Sanctions

- Workforce members and agents will be trained on how to identify and report breaches within JSSA. JSSA will apply appropriate sanctions in accordance with JSSA's progressive disciplinary procedures against workforce members and agents who fail to comply.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Security Management Process

The HISO, in conjunction with the PO, is responsible for assessing potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI, including electronic PHI, maintained by JSSA. The HISO is responsible for implementing appropriate security measures to reduce identified risks and vulnerabilities. The HISO and PO will work in collaboration as necessary.

Risk Analysis & Risk Management

The HISO will conduct a risk assessment on an annual basis. The HISO also will conduct a risk assessment when there is a material change in JSSA's operating environment or business practices that may reasonably implicate the confidentiality, integrity, or availability of PHI maintained by JSSA.

Risk assessments will identify potential security risks, evaluate the likelihood of security risks occurring, and estimate the magnitude of risk associated with the identified security risks. The risk assessment also will evaluate the extent to which JSSA's existing HIPAA Policies and Procedures meet all of HIPAA's requirements.

The HISO and PO will take appropriate action to correct identified vulnerabilities. Corrective action may include:

- Revising JSSA's HIPAA Policies and Procedures;
- Modifying the HIPAA compliance training program; and
- Disciplining workforce members for violations of these policies.

The results of all risk assessments, as well as follow-up actions taken to correct identified deficiencies, will be documented. The PO will maintain this documentation for six years.

Information System Activity Review

The HISO will implement procedures to regularly review records of information system activity, including the creation of audit logs, access reports, and security incident tracking reports. The HISO will develop criteria to determine the information system activities to be audited. Records will be maintained regarding the identity of JSSA workforce members who access or attempt to access systems containing PHI, as well as the identity of workforce members who create or modify data in any of JSSA's databases containing PHI.

The HISO will inform the PO of any unusual activity identified by the regular review of information system activity.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Access Authorization

Access authorization, modification and termination is the process of determining whether an individual should be granted access to JSSA's data and the process of modifying and terminating access to data. An authorized workforce member is a person who has been granted explicit authorization and access to JSSA's data.

I. <u>Granting Access</u>

Human Resources, or designee, will submit an authorization of access notice in the following situations:

- When the employment or other arrangement with staff begins and access to ePHI, or areas where ePHI is accessible, is required to perform their responsibilities to JSSA (e.g., new hire, new business associate, etc.)
- When staff which had no prior access, now requires access to ePHI, or areas where ePHI is accessible, in order to perform their responsibilities to JSSA (e.g., transfer, promotion, etc.)
- When existing access to ePHI, or areas where ePHI is accessible, for staff should be modified due to a change in their responsibilities to JSSA (e.g., transfer, promotion, etc.)

  The HISO and Human Resources, or designee, will determine which workforce members get access to data. In making such determinations, the HISO or designee will follow these guidelines:
  - Workforce members will not be granted access to PHI unless they have a need for access.
  - Workforce members will get access to only the minimum amount of PHI (and types of PHI) needed to perform their duties.

  Consideration will be given to situations in which staff might be able to approve their own access privileges by requiring a second person to approve the access authorization.

- HISO's designee will provide access and monitor levels of access, as appropriate. All prospective workforce members will receive required training.

- HISO's designee will:
  - Suspend access, when appropriate, to respond to a breach of confidentiality/security in coordination with JSSA's Breach Notification Policy.
  - Modify access when notified to do so in accordance with the modification procedure, set forth below.
  - Terminate access when notified to do so in accordance with the termination procedure, set forth below.

- Authorized workforce members with access to PHI must comply with the following requirements:
  - Use the data only for purposes authorized by JSSA.
  - Comply with all JSSA HIPAA Policies and Procedures governing PHI.
  - Not disclose data unless authorized to do so.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

II. Modifying Access

- The HISO and Human Resources, and in collaboration with the PO as necessary, shall determine if an individual or a group of individuals need more, less, or otherwise modified access because of a change in duties or a change in status.

- When the PO makes a determination that a modification is necessary, the PO shall request that the HISO or designee modify access.

III. Terminating Access

- Human Resources is responsible for notifying the appropriate staff, including the HISO and PO or designee, that an individual will no longer need access to data (whether because the workforce members employment or other arrangement with JSSA has ended or because of any other reason).

- Any other workforce member who becomes aware that an authorized workforce member is leaving JSSA permanently or for an extended or unexplained absence should report the matter to Human Resources and the HISO for a determination of whether to terminate access.

- Upon termination of an authorized workforce member's access, the HISO or designee, and Human Resources will immediately take the following actions:
    - Terminate access privileges, including usernames and passwords, to system and data resources and secure areas.
    - Retrieve sensitive materials, including access control items such as keys and badges.
    - Retrieve all hardware, software, data, and documentation issued to or otherwise in the possession of the authorized workforce member.
    - Arrange an exit briefing to verify retrieval of all items, discuss any security/confidentiality concerns, and remind the authorized workforce member of the continuing need to protect data security and client/patient confidentiality.
    - Maintain records of the termination procedure for each authorized workforce member, including the retrieval of security-related items, such as badges, passwords, and information system assets, for not less than six (6) years from the termination date.

- When necessary, Human Resources or designee will escort terminated workforce members from JSSA and arrange for an immediate audit of their accounts to detect any security or confidentiality threats or breaches.

IV. Responsibilities

JSSA's Human Resource Department is responsible for items including, but not limited to, the following:

- Requesting access for staff only after proper clearance.
- Requesting access for staff only if their job responsibilities require access.
- Requesting only that access which is appropriate for their role and is necessary to perform their job responsibilities (minimum necessary access).
- Requesting access to be modified for staff immediately when there is a change in their job responsibilities (e.g., transfer, promotion, etc.).

©2026 JSSA. All rights reserved. Proprietary to JSSA.

- Ensuring job descriptions accurately reflect assigned duties and responsibilities and outlining access requirements.

JSSA's Information Technology (IT) Department is responsible for items including, but not limited to:

- Creating and modifying access to ePHI (including remote access, if applicable) per the Information Access Management policy.
- Tracking and logging the issuance of JSSA owned electronic devices (e.g., desktops, laptops, tablets, cell phones/smartphones, printers, removable storage devices, routers, switches, cellular wireless modems/air cards/jetpacks, etc.) along with any applicable identification numbers (e.g., asset tag number, serial number, etc.) per the Device and Media Controls Policy.
- Ensuring job descriptions accurately reflect assigned duties and responsibilities and outlining access requirements and authorization to grant access.
- Enforcing segregation of duties to prevent situations where staff might be able to approve their own access privileges by requiring a second person to approve the access authorization.
- Issuing physical access controls (e.g., keys, electronic door access cards, identification (ID) cards, etc.) and modifying access per the Facility Access Controls policy.
- Tracking and logging the issuance of JSSA physical access controls per the Facility Access Controls policy.
- Ensuring job descriptions accurately reflect assigned duties and responsibilities and outlining access requirements and authorization to grant access.

V. Documentation

JSSA's IT Department or designated staff will log, track, securely maintain, and retain documentation for each authorization of access notice for six (6) years from the authorization date of submission including, but not limited to, the following:

- Full name, title, and department of person submitting the authorization of access notice.
- Full name, title, department, job role, access requested/access modification requested (and reason), and the access request start date for the employee in which access is to be granted or modified.
- Date and time the authorization of access notice was submitted to the appropriate department.
- Date and time the authorization of access notice was received by the receiving department.
- Full name, title, and department of person fulfilling the authorization of access notice.
- Date, time, and description of actions taken/access granted or modified during the fulfillment of the authorization of access notice.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Information System Security

The HISO is responsible for providing security awareness and training to all JSSA workforce members and preventing unauthorized access to JSSA's information systems. The HISO is responsible for the day-to-day operation of the Information System Security Policy.

Method for Accessing JSSA's Information System

Each JSSA workforce member granted access to JSSA's information system pursuant to the Access Authorization Policy will be assigned a unique username to use in accessing JSSA's information system. JSSA's information system will be accessible only by a workforce member using the workforce member's username in conjunction with a password personally selected by the workforce member. Passwords must be securely maintained and may not be shared.

Security Training & Reminders

Training will be provided to all workforce members on applicable access limitations and security training. JSSA also will provide periodic retraining to workforce members as needed, including providing formal retraining on security policies and procedures to any workforce member who has been identified as violating JSSA's information security policies or any other workforce member who requests retraining. The training will instruct workforce members on how to help guard PHI maintained in JSSA's information system, including training on protecting against malicious software, system protection capabilities, log-in procedures, and password protection procedures.

JSSA will provide periodic security updates relating to the security of its information system. The periodic security updates will be provided to all workforce members, including management, with access to JSSA's information system. The security updates will take the form of email notices, printed notices, discussion topics for monthly staff meetings, and information posted to the JSSA intranet.

The HISO or designee will maintain documentation of periodic security updates provided to workforce members for six years from the date the periodic security update was provided or implemented. The documentation will include the type of reminder, its message, and the date it was implemented.

Prevention of Unauthorized Access to JSSA's Information System

Any workforce member who detects or suspects a security problem relating to PHI or JSSA's information system, such as a suspicion that JSSA's information system has been corrupted by malicious software, JSSA's information system or PHI maintained by JSSA has been accessed by an unauthorized individual or has been accessed for an unauthorized purpose, or a JSSA facility or location within a facility containing PHI is not secure, must report this suspicion immediately to the PO and/or the HISO.

The reporting workforce member should follow up immediate notification with a written incident report that includes the following information:

- Narrative of the security problem; and
- Estimate of how long the problem may have existed.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

JSSA workforce members will comply with the security requirements of this policy and all other applicable information privacy and security policies.

Protection from Malicious Software

The HISO will implement reasonable measures to protect JSSA's information system from unauthorized access by third parties. These measures will include, but are not limited to, the following:

- Installing intrusion detection software to detect unauthorized access;
- Ensuring that all information systems have reasonably up-to-date firewall protection and operating system security patches designed to maintain the integrity of PHI maintained on the information system; and
- Ensuring that all information systems have reasonably up-to-date versions of system security agent that includes malware protection and reasonably up-to-date patches and virus definitions.

Log-In Monitoring

The HISO also will monitor attempts to log-in to its information system and will have systems in place to identify multiple unsuccessful log-in attempts and to create an audit trail of log-in attempts. If a workforce member's username is associated with three consecutive unsuccessful log-in attempts, the workforce members password will be required to be reset. The HISO or designee will be informed of any required password reset, and a new password will be provided to the workforce member only with the HISO's or designee's approval.

Password Management

JSSA's workforce members are responsible for maintaining the security of their information system passwords. Each workforce member will comply with the following guidelines:

- Workforce members logging onto the system will ensure that no one observes them entering their password;
- Passwords must be memorized and may not be written down. Multiple passwords may be recorded electronically only using a method approved by the HISO;
- Passwords will not be disclosed to another individual or entity, either inside or outside of JSSA;
- Passwords will not be transmitted online, particularly by email;
- Workforce members will not allow another individual to access the information system through the use of the workforce member's password without HISO's approval;
- Workforce members will not access the information system through the use of another workforce member's password; and
- Any other guideline that the HISO determines would prevent putting the availability, accuracy, or confidentiality of JSSA data, media, or equipment at risk.

JSSA will maintain an audit log of workforce member activity, and a workforce member will be considered responsible for any activities performed on the information system by any individual using the workforce member's username and password.

Failure to comply with these password management policies will result in disciplinary action, up to and including termination, in accordance with JSSA's Progressive Discipline Policy.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Security Incident Procedures

The HISO is responsible for responding to any instances of unauthorized information system activity. The HISO will provide the PO with all necessary information for investigative purposes and the HISO is responsible for the day-to-day operation of the Security Incident Procedures policy.

Response and Reporting of Security Incident Procedures

In accordance with its policies, JSSA will implement procedures to regularly review records of information system activity in order to detect an attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in JSSA's information system ("Security Incident"). Security Incidents include, but are not limited to, the unauthorized accessing of PHI through the information system and incidents, such as theft of a computer, involving media on which PHI is stored.

The HISO and PO will be informed of all Security Incidents that result in a successful unauthorized access, use, disclosure, modification, or destruction of PHI. The HISO also will be informed of any pattern of Security Incidents, even if the Security Incidents do not result in the successful unauthorized access, use, disclosure, modification, or destruction of PHI.

All Security Incidents will be investigated. All Security Incidents involving a breach of unsecured PHI will be responded to in accordance with the Breach of Unsecured PHI Policy. Security Incidents will be documented in a log by the PO describing each event, the person responsible (if known), actions taken in response, and other pertinent information. The PO will maintain this documentation for six years from when the security incident occurred or was discovered, whichever is later.

JSSA will take steps to mitigate, to the extent practicable, harmful effects of Security Incidents that are known to it.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Contingency Plan

The PO and HISO are responsible for ensuring that JSSA's HIPAA Policies and Procedures are in place for responding to an emergency or other occurrence, such as fire, vandalism, system failure, and natural disaster that damages systems containing electronic PHI. The HISO is responsible for the day-to-day security operations of this HIPAA Policy.

Preparation for Emergencies

I. Data Backup

JSSA will back up its information system network to help achieve the goal of protecting data integrity, confidentially, and availability in the case of an emergency.

- The HISO is responsible for performing daily, automated backups on JSSA's network, including shared drives containing application data, client/patient information, financial data, and crucial system information.
- All data captured in the backup will be replicated to an off-site location each night as part of JSSA's overall disaster recovery plan.
- The HISO, the system administrator, or their designees will monitor the backup jobs to validate the accuracy, completeness, and integrity of the backup performed the previous night.
- The HISO, the system administrator, or their designees will immediately act upon any errors. Responsible workforce members will use contract technical support as needed to resolve problems and ensure the validity of backup data.
- The HISO will periodically test the ability to restore data in the event of a computer system problem, failure, or other disaster to ensure data integrity, availability, and confidentiality.

II. Protection of JSSA Network

The HISO is responsible for installing electrical power protection devices to suppress surges, reduce static, and otherwise protect JSSA's information system network, including its workstations. The HISO will ensure that a system is in place to provide backup power to JSSA's information system network in the event of a power failure.

III. Revision of Emergency Response Plan

On an annual basis, the HISO will review and update JSSA's Emergency Response Protocols and Disaster Recovery Plan to ensure that they contain adequate provisions for allowing facility access in support of restoration of lost data, restoring lost data, ensuring the continued security of electronic PHI during emergency operations, providing access to required electronic PHI during the emergency, and otherwise responding to events that damage systems containing electronic PHI. As part of this review, the HISO will ensure that the Protocol and/or Plan contain an up-to- date assessment of the relative criticality of the applications and data needed to support JSSA's contingency plans and that provisions have been made to ensure that the critical applications and data will be available if an emergency occurs. The HISO will ensure that the Protocol and Plan are revised, as necessary.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

IV. Emergency Response

If an emergency or other occurrence that damages systems containing electronic PHI takes place, the HISO will be responsible for regulating facility access in support of restoration of lost data, restoring lost data, ensuring the continued security of electronic PHI during emergency operations, providing access to required electronic PHI during the emergency, and otherwise responding to the event in accordance with the provisions of JSSA's Emergency Response Protocols and Disaster Recovery Plan.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Facility Access Controls

JSSA is committed to maintaining the security of PHI in its possession. In keeping with this commitment, physical access to JSSA facilities and to locations in JSSA's facilities in which paper or electronic copies of PHI are stored or from which PHI can be accessed is restricted to authorized workforce members and is permitted only for the purpose of conducting business that fulfills JSSA's mission.

Physical Access Authorization, Modification, and Termination

- The PO, HISO and Human Resources, are responsible for determining the degree of access that each JSSA workforce member and visitor has to JSSA facilities and to locations within the facilities, such as computer rooms and client/patient record storage rooms.
- Physical access authorization, modification, and termination for JSSA workforce members will be determined in accordance with the Access Authorization Policy.
- A secure system for physical and electronic keys and badges will be maintained to ensure security of keys and badges. This secure system includes storage of keys in a locked room with restricted access controls. If there is a breach, each compromised lock will be changed.
- A visitor control policy must be maintained to ensure that access to JSSA facilities by clients, visitors and the general public is secure.
- Per all applicable JSSA policies and procedures, all workforce members must be escorted from the building by a JSSA Human Resources staff member or department head on their last day of employment.
- Upon termination of employment with JSSA, all physical and electronic keys must be returned and disabled.
- Former JSSA workforce members are subject to JSSA's Visitor Control Policy.

Physical Access to JSSA Facilities

All methods of entry and exit to JSSA facilities must be secured with mechanical and/or electronic locks.

- Primary entrances to each facility must have a system of electronic locks and badges for staff to enter the building. Each badge must have a unique identifier associated with the staff person that is authorized to enter.
- Secondary entrances including "exit only" doors, mechanical doors, and electrical room doors require physical locks only. These doors must be kept locked at all times.
- Security cameras will monitor building entrances to deter/detect unauthorized entry.

The Facilities Manager will maintain documentation of all repairs and modifications made to the physical components of a JSSA facility that are related to the security of the facility.

- Documentation will be maintained of all routine maintenance checks, repairs, and modifications related or made to security devices (such as security cameras), fences, walls, doors, and locks, as well as any other relevant physical components.
- Documentation will include the date, reason for repair or modification, and the individual who authorized the activity.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Physical Access to Locations Within JSSA Facilities

Rooms with restricted access will be locked at all times when room is not in use. Access to such rooms will be limited to workforce members who require access for the normal performance of their duties. Doors must not be left open and unattended for any period of time. Doors must not be propped open. When leaving restricted areas, staff must ensure the door is properly closed and locked.

Physical client/patient records temporarily stored outside of storage rooms must be secured in a locked file cabinet in a locked room. All other types of physical records must be stored in a locked room.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Workstation Set-up and Use

Workstation Locations

Computers from which PHI can be accessed will be placed in secure areas. No computers will be located in areas that are accessible by client/patient or the general public in the absence of a JSSA workforce member.

- Access to computer rooms will be limited to workforce members who require access for the normal performance of their duties.
- Computer rooms will be securely locked when unattended.

Workstation Area Set-up

- Computer monitors will, when possible, be positioned so that unauthorized individuals cannot view the information on the screen.
- Computer monitors that are potentially visible to unauthorized workforce members will be equipped with privacy screens.
- Each computer will be programmed to logoff or generate a password protected screen saver that locks the computer screen when the computer receives no input for 15 minutes.

Workstation Use – Protection of JSSA Information Network and PHI

All workforce members will take appropriate measures to protect computers and data (both electronic and hard copy) from harm and from exposure to unauthorized individuals. This policy applies to the use of both personal and JSSA provided equipment, including desktop PC's, Laptop Computers, tablets (including iPad), Mobile Phones, etc. This also applies to work areas including offices, desk areas and other common work areas.

- Workforce members logging onto the system will ensure that no one observes them entering their password.
- Workforce members will maintain the security of their information system passwords pursuant to the Information System Security Policy.

Workforce members using the computer system will not write down their password and put it at or near the terminal, such as by putting the password on a yellow "stickie" on the screen or a piece of tape under the keyboard.

Workforce members will not log onto the system using another's password nor permit another to log on with their password. Nor will workforce members enter data under another person's ID and password.

Each person is responsible for the content of any data he or she inputs into the computer or transmits through or outside the system. No person may hide his or her identity as the author of the entry or represent that someone else entered the data or sent the message. All workforce members will familiarize themselves with and comply with JSSA's Email Policy.

- After three failed attempts to log on, the system will refuse to permit access.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

- Workforce members must lock their workstation screen using the Ctrl-Alt-Del keyboard command when a client/patient or visitor is in the same office or location. Screen must remain locked for the duration of the session.
- Workforce members must log out or lock their workstation screen using the Ctrl-Alt-Del keyboard command before leaving their workstation unattended.
- Workforce members must not leave printers unattended when they are printing confidential client/patient or other information, especially when two or more computers share a common printer or when the printer is in an area where unauthorized workforce members have access to the printer.
- Workforce members must not leave workstation areas or other work areas unattended without first securing all PHI in the area, including file folders, client/patient records/charts, and other papers.

Whenever possible, workforce members must lock their work areas, including cabinets, storage shelves, and office doors. Workforce members must not leave clients/patients or visitors unattended in their work areas.

- Workforce members will not permit anyone else to use the computer for any purpose, including, but not limited to, a workforce member's family and/or associates, clients/patients, client/patient families, or unauthorized officers, other workforce members, contractors, and agents of JSSA.
- Workforce members must ensure that all PHI being transported from one work area to another is not left unattended including in such en-route locations as other offices, common areas, restrooms, etc.

Workstation Use – General Use Guidelines

- No workforce member may access any confidential client/patient or other information that they do not have a need to know. No workforce member may disclose confidential client/patient or other information unless properly authorized.
- No workforce members may upload or download any unauthorized software or data including games, music applications (iTunes; Pandora or other "streaming" music players), web browser tool bars, weather tracking applications, etc. The HISO must approve any software or data that a workforce member wishes to upload or download. This rule is necessary to protect against computer viruses from being transmitted into JSSA's information system.
- Workforce members will access the internet from JSSA workstations and through JSSA's information system only in a manner consistent with the requirements of JSSA's Internet Security Policy.
- Loss/theft/damage of JSSA equipment must be reported immediately to the HISO. Loss or theft of personal equipment connected to JSSA's network must also be reported immediately to the HISO per JSSA's Mobile Phone Policy and Laptop Policy.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Internet Security

JSSA workforce members who use JSSA's system for internet access must comply with this policy for all internet access, communications, and storage using JSSA's system. JSSA's business information, information system networks, and PHI can be placed at risk by inappropriate or unauthorized internet use. Accordingly, workforce members will access the internet for business purposes only in order to help ensure the integrity, security, and confidentiality of JSSA's systems, PHI, and other sensitive data. All internet access also will occur in accordance with the requirements of JSSA's HR Electronic Systems Usage Policy.

All workforce members must strictly observe the following rules when using the internet:

- Workforce members must have a business purpose for any access and use of the internet.
- Workforce members may not access or use the internet for personal business or personal commercial gain.
- To protect the integrity and security of JSSA's information systems, workforce members may not access pornographic or other offensive websites, including, but not limited to, sexist, racist, discriminatory, hate, or other sites that would offend a reasonable person in the same or similar circumstances. If the workforce member has any doubt whether access to a specific site is proper, he or she should seek approval from his or her department director.
- Access control:
    - Workforce members may not use any other workforce member's password or other identification to access the internet.
    - Workforce members attempting to establish a connection with JSSA's computer system via the internet must authenticate themselves before gaining access to JSSA's internal network.
- PHI will be transmitted over the internet only in accordance with all applicable JSSA policies regarding the use or disclosure of PHI.
- JSSA reserves the right to audit internet access in accordance with JSSA's policies at any time and without prior notice.
- No workforce member may attempt to probe computer security mechanisms at JSSA or other internet sites unless part of an audit approved by the HISO.
- Workforce members will immediately report security problems with internet use, breach of confidentiality, and any violations of this or other JSSA policies and procedures occurring during internet use in accordance with the applicable JSSA policies and procedures.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Portable Computer and Mobile Device Use

JSSA workforce members who use or disclose PHI on portable computers or mobile devices, such as mobile phones, must comply with the applicable provisions of the Workstation Set-up & Use Policy, the Internet Security Policy, and any other relevant policy, as well as with the additional procedures described below.

Portable Computers

- JSSA will provide portable computers to workforce members based on approved business needs. Workforce members agree to use the equipment solely for JSSA's business purposes.
- No workforce member may, for any purpose, download, forward, maintain/store, or transmit confidential client/patient or other information on a personal/and or portable computer.
- The hardware, software, all related components, and data are the property of JSSA and must be safeguarded and be returned upon request and/or upon termination of employment.
- For JSSA supplied equipment, workforce members further understand that:
    - Remote access functions are restricted to JSSA systems only.
    - Workforce member is not permitted to connect to any other unauthorized services, internet service providers, or any other internet access in any other manner.
    - Workforce member will not download any software onto the computer except as loaded by authorized staff of the HISO.
    - Workforce member will not insert Flash (Thumb) Drive, CDs, DVDs, or any other media into the computer without the authorization of the HISO.
    - Workforce member must use only batteries and power cables provided by JSSA.
    - Workforce member is responsible for securing the unit, all associated equipment, and all data within homes, cars, and other locations.
    - Workforce member may not leave mobile computer units unattended unless they are in a secured location.
    - Workforce member must place portable computers and associated equipment in their proper carrying cases when transporting them.
    - Workforce member must not alter the serial numbers and asset numbers of the equipment in any way.
    - Workforce member will not permit anyone else to use the computer for any purpose, including, but not limited to, the workforce member's family and/or associates, clients/patients, client/patient families, or unauthorized officers, other workforce members, and agents of JSSA.
    - Workforce member must not share passwords with any other person, must safeguard passwords, and may not write them down so that an unauthorized person can obtain them.
    - Workforce member must report any breach of password security immediately to the HISO.
    - Workforce member must maintain client/patient confidentiality when using the computers, as specified in JSSA's Workstation Set-up & Use Policy. The workforce member must protect the screen from viewing by unauthorized workforce members, and the workforce member must properly log out and turn off the computer when not using it.
    - Workforce member must immediately report any lost, damaged, malfunctioning, or stolen equipment or any breach of security or confidentiality to the PO and HISO.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Mobile Phones and other Mobile Devices

- Use of mobile phones and other mobile devices are subject to JSSA's Mobile Phone Policy and Laptop Policy.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Off-Site Work

Maintaining Confidentiality of PHI

For each off-site location defined below, the workforce member is responsible for ensuring that no other party at the location has access to the PHI. The workforce member must take extra precautions such as logging out or locking the screen after every use on the computer. Any workforce member who does not follow this policy may be subject to disciplinary action. ALL HIPAA requirements apply at all times when accessing client PHI regardless of location. Off-site locations include:

- **Home Location** – Workforce member's primary residence.

- **Other Private Location** – Areas outside the home including, but not limited to, hotel rooms, family member homes, client/patient homes, and other similar private locations.

- **Public Location** – Workforce member is **NOT** permitted to work in any public location, including, but not limited to, restaurants, airports, airplanes, cafes, hotel lobbies, hotel business centers, libraries, or other public areas, where the workforce member cannot ensure that no other party in his/her location has access to the PHI.

Workforce members who work off-site are subject to all JSSA rules, policies, and procedures applicable to those who work for JSSA, including, but not limited to, time and attendance, leave, insurance and other benefit, and JSSA's HIPAA Policies and Procedures.

Security of PHI

Under no circumstances should PHI be downloaded, stored, or saved on the workforce member's JSSA assigned computer or personal computer or other device.

Unless explicitly authorized by the PO, hard copies of any part of the client/patient record may not be removed from JSSA premises. Materials, documents, computers and so forth transported to or from the off-site location are the workforce member's responsibility. The workforce member will protect JSSA records and documents from loss, damage, theft, unauthorized access, use, or disclosure. Conditions for offsite use of personal information assets such as a personal computer or similar device include the following:

- Data, media, supplies, or information assets of JSSA are not to be used for private purposes or for unauthorized reasons, such as unapproved research.
- When such assets are off the premises of JSSA, they must be under the care and control of the person authorized to remove and use the assets.
- Workforce members must immediately report all losses of or damage to such equipment to the HISO. Breaches of confidentiality and other reportable incidents resulting from loss or damage of such equipment must be reported in accordance with JSSA's Breach of Unsecured PHI Policy.
- Workforce members will use appropriate safeguards for all assets as required by the HISO. Assets, such as computers, mobile devices, etc. must not be left unattended. Workforce members must secure media in appropriate locations, such as a locked cabinet.
- JSSA's Portable Computer and Mobile Device Use Policy supplements this HIPAA Policy for such assets.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Device and Media Controls

Device and Media Tracking

The HISO will develop and maintain an inventory of hardware and electronic media that contain or can access PHI. The inventory will include a current location of equipment or, in the case of portable devices (e.g., portable computers, mobile phones), the name of the workforce member who has possession of the device.
Hardware and electronic media may not be removed from a JSSA facility or moved to a new location within a JSSA facility without the consent of the HISO. Consent may consist of a blanket authorization for certain workforce members to remove and use such assets offsite.

Before authorizing the movement of hardware and/or electronic media that contain PHI, the HISO will determine whether risk exists that the PHI will be damaged during the movement of the equipment. If this risk exists, then a retrievable, exact copy of the PHI will be made before the equipment is moved. The movement of equipment that permits access to PHI on JSSA's information system but does not contain PHI does not pose a risk that the PHI will be damaged during the movement of the equipment.

Destruction of PHI

JSSA, its workforce members, and agents may destroy data only in accordance with JSSA's Records Retention and Destruction Policy. Data that is involved in an audit, investigation, or litigation will not be destroyed.
All computer desktops, laptops, hard drives, and portable media must be processed through the HISO for proper disposal.

The PO must approve any non-routine destruction of PHI. The PO will maintain documentation of the non-routine destruction of PHI for no less than six (6) years.

- Routine destruction of PHI includes the destruction of paper containing PHI not associated with the client record, including, but not limited to, copies of authorizations, personal notes, emails, and faxes, and paper containing any other type of confidential or private information not deemed to be part of the permanent record.
- Non-routine destruction of PHI includes the destruction of paper containing PHI associated with the client record; paper involved in an audit, investigation, or litigation; and paper associated with accounting and governance.

JSSA will destroy any item containing PHI, including electronic PHI, in such a manner that the PHI is unusable and/or inaccessible before disposing of the item.

- Paper, film, or other hard copy records containing PHI will be shredded or otherwise destroyed so that the recorded PHI cannot be reconstructed. Redaction is not an acceptable means of data destruction.
    - Records should be shredded using a shredder approved by the PO.
    - Commercial shredding of paper records may be authorized only by the PO.
- Electronic media will be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, so that the recorded PHI cannot be retrieved.
    - Computers, hard drives, and other electronic media (thumb drives, flash drives, etc.) must be returned to the HISO for proper disposal.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

The PO is responsible for ensuring that destruction services contractors have signed business associate agreements before providing destruction services.

See JSSA's Record Retention and Destruction Policy for additional information.

Media Re-Use

Electronic media that has stored PHI may be reused, but only after all PHI previously stored on the media has been removed consistent with this HIPAA Policy.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Encryption and Decryption

Encryption Policy

JSSA will encrypt:

- All transmitted records and files containing PHI that will travel across public networks;
- All data containing PHI that will be transmitted wirelessly;
- All PHI stored on laptops or other portable devices, including mobile phones; and
- All emails containing PHI.

PHI also may be encrypted in other situations on a case-by-case basis.

Encryption Standard

Information will be considered encrypted when the following conditions are met:

- Data has been transformed through the use of a 128-bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key.
- The confidential process or key has not been breached. In order to prevent a breach, the process or key will be stored on a device or at a location separate from the data it is used to encrypt or decrypt.
- The algorithmic process used is one of the encryption processes identified by the U.S. Department of Health and Human Services, Office for Civil Rights as rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals for the purposes of the Breach Notification Rule.

Exception to Encryption Requirement

The PO or HISO may permit case-by-case exceptions to this policy for the transmission of PHI to business associates or other authorized recipients of PHI when the business associate or other recipient does not use a compatible encryption technology. Before granting such an exception, the PO or HISO will ensure that alternative methods for ensuring the security of the PHI have been implemented.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Information Integrity

The HISO is responsible for ensuring data quality and data integrity for PHI and other information maintained on JSSA's information system network. All JSSA workforce members are responsible for reporting problems with data integrity or suspected or actual breaches of data security to their department directors, PO, and/or the HISO.

Data Integrity

The HISO will implement appropriate electronic mechanisms to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner. These mechanisms will include mechanisms to ensure that electronic PHI is not improperly modified during transmission.

Appropriate mechanisms will be implemented based on risks to the integrity of electronic PHI identified during the annual risk assessment performed in accordance with the Security Management Process Policy.

- Consistent with the Security Management Process Policy, appropriate mechanisms will include audit logs, access reports, and security incident tracking reports that identify JSSA workforce members who access or attempt to access systems and files containing PHI, when access occurred, and for how long the access continued. The information tracked will include logins and logouts, accesses or attempted accesses to files or directories, creation or modification of data, execution of programs, and uses of peripheral devices.

Department directors are responsible for advising the HISO and/or the PO of required data integrity standards for data that they maintain, use, and transmit and any problems with data integrity.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Appendix A: Additional Resources

Statement of Acknowledgment and Agreement: Orientation and Annual
Statement of Acknowledgement and Agreement for HIPAA and Sending Secure Emails
Statement of Acknowledgement and Agreement for Hospice Volunteers
Authorization to Release Information form
Client Request for Information form
Designation of Authorized Representative and Release of Information form
Liability and Publicity Release form
Media Filming Authorization form
Notice of Privacy Practices
Client Rights and Responsibilities
Consent for Telehealth and Telemedicine
Business Associate Agreement

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Appendix B: HIPAA Policy and Procedure Definitions

JSSA
Jewish Social Service Agency

Workforce Member
Employees (full-time, part-time, hourly), volunteers, interns, contractors, board members, temporary staff.

Business Associate
A person or organization that conducts business with the covered entity that involves the use or disclosure of individually identifiable health information.

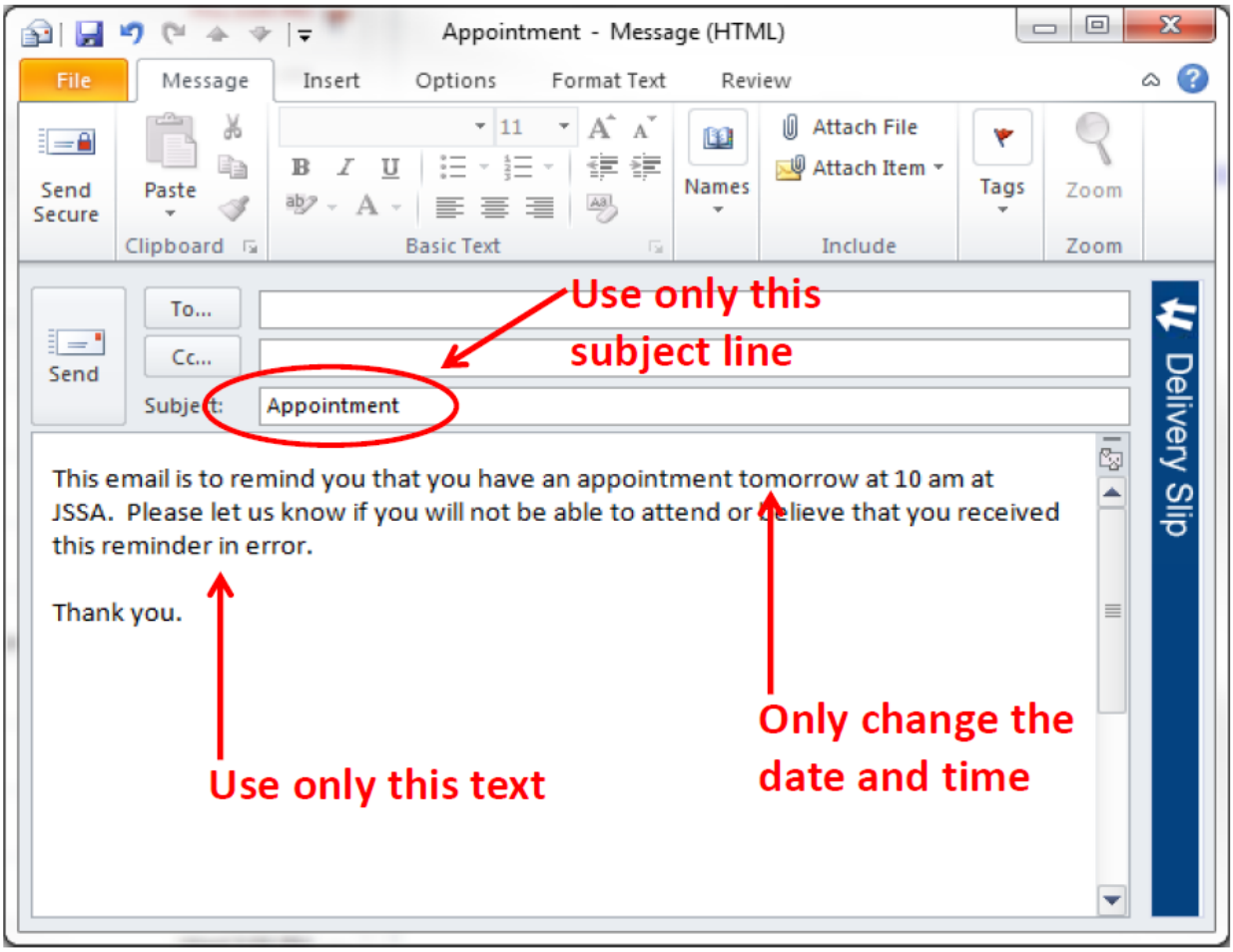
PHI
Protected Health Information

Direct Service Provider
JSSA workforce members who provide services (clinician, nurse, case manager, etc.) directly to the client.

Substance Use Disorder (SUD) Records:
Records that identify an individual as having or having had a substance use disorder and that are subject to the confidentiality requirements of 42 CFR Part 2. Such records may include diagnosis, treatment, referral, or payment information related to substance use disorder services and are subject to additional federal confidentiality protections beyond HIPAA.

©2026 JSSA. All rights reserved. Proprietary to JSSA.

Appendix C: Appointment Reminder Template



©2026 JSSA. All rights reserved. Proprietary to JSSA.

Appendix D: Version Control

Version Number	Date	Applicable Section	Comments	Approver/Todd Schenk, CEO
V.1	02/15/15	Entire Policy	Minor Revisions, corrections per compliance officer	
V.1	04/08/16	Entire Policy	Reviewed, no changes	
V.1	06/22/17	Entire Policy	Reviewed, no changes	
V.1	01/30/18	Entire Policy	Reviewed, proposed changes to be reviewed at later date	
V.1	01/29/19	Entire Policy	Reviewed against proposed regulations, no additional changes to be considered	
V.1	07/03/19	Entire Policy	Reviewed, proposed changes to be reviewed at later date	
V.1	02/18/20	Entire Policy	Reviewed; proposed policy updates underway	
V.1	07/15/21	Entire Policy	Reviewed, Individual IT Policies Updated; proposed policy updates underway	
V.2	10/27/22	Entire Policy	Updated format, procedures, reporting protocols.	
V.3	02/15/23	Entire Policy	Reviewed: individual policies updated; removed PHC language; formatting, updated HISO and PO responsibilities.	
V.3	02/15/24	Entire Policy	Reviewed, no changes	
V.3	02/25/25	Entire Policy	Reviewed, no changes	
V.4	1/26/26	Entire Policy	Updated SUD language to comply with 42 CFR Part 2.	

©2026 JSSA. All rights reserved. Proprietary to JSSA.