

PANHANDLE HEALTH DISTRICT POLICY

Policy - Minimum Necessary/Protected Health Information Policy Covers: HIPAA Compliance, Client Confidentiality and Privacy	Policy No. General Policy 1-5 Effective: 3/26/03
--	---

Policy: It is the policy of Panhandle Health District (PHD) to ensure that only the minimum necessary Protected Health Information (PHI) is used, disclosed, or requested in Treatment, Payment or Operations (TPO) at PHD.

PHD will ensure the privacy and confidentiality of patient and client information entrusted to the Health District's care. PHD will ensure that the release of all information is in strict conformance with state and federal statutes, Health Insurance Portability and Accountability Act (HIPAA) regulations, and ethical practices.

This policy applies to all employees, volunteers, students and those under contract who are business associates with PHD. All employees, upon employment, acknowledge receipt and understanding of this policy by completing the online review of required policies within 30 days of employment. Volunteers and students acknowledge receipt of this policy by signing the Volunteer Agreement ([Volunteer Policy 3-4](#)) acknowledging that they have received and read the Minimum Necessary/Protected Health Information Policy 1-5. The signed acknowledgement forms will be maintained in the PHD Human Resources office.

The following protocols (click on links to each protocol) will be utilized as resources in PHD's HIPAA initial and periodic training:

- [Protocol 1-5A HIPAA Compliance](#)
- [Protocol 1-5B HIPAA Information and Procedure Manual](#) (SharePoint/District Policies and Procedures/HIPAA)
- [Protocol 1-5C HIPAA Training and Testing](#)
- [Protocol 1-5D Confidentiality](#)
- [Protocol 1-5E Requests for PHI and Release of PHI](#)
- [Protocol 1-5F Sanctions on Violations](#)
- [Protocol 1-5G Electronic Protected Health Information Procedure](#)
- [Protocol 1-5H After Hours Entry into Hayden Building](#)
- [Protocol 1-5I Photography, Video and Electronic Imaging or Recording](#)

Revision No.: 11 Reviewed: 4/7/22 No Changes Revision Date: 8/13/20	Issued by: //Lora Whalen//
---	-------------------------------

Protocol 1-5A: Health Insurance Portability and Accountability Act (HIPAA) Compliance

PHD will ensure compliance with the Standards for Privacy of Individually Identifiable Health Information ([45 CFR, part 160 and part 164, HIPAA](#)).

1. Definitions for HIPAA Compliancy

- a. **HIPAA** - Health Insurance Portability and Accountability Act of 1996. It contains provisions for protecting the privacy of patient Protected Health Information (PHI).
- b. **Patient** - An individual who seeks medical treatment, is provided with medical treatment, or provides health information (for example, when a new patient requests a first appointment) or a specimen such as blood or urine.
- c. **Protected Health Information (PHI)** - Individually identifiable information in any form (including written, auditory, or electronic information) or format that:
 - Is contained in a document that can be transmitted electronically or maintained in any other form;
 - Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearing house;
 - Is related to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual; or the past, present or future payment for provision of health care to an individual;
 - Contains, but not necessarily limited to, a diagnosis, prognosis, treatment or therapy notes, medical/psychological consultations, recommendations, referrals; physician or physician assistant, nurse practitioner, nurse, social worker, or any other licensed medical or psychological practitioner notes;
 - Contains medications or prescriptions for medications, medical or psychological test results of any kind;
 - Contains personal information collected in conjunction with receiving medical advice or treatment such as income, family status, or information pertaining to sexually transmitted disease contacts.
- d. **Covered Entity** – A covered entity is a health plan, a health care clearinghouse or a health care provider who transmits any health information in electronic form in connection with a transaction for which the Secretary of Health and Human Services has adopted standards under HIPAA.
- e. **Business Associate** - A HIPAA Business Associate is a person who on behalf of PHD, but other than an employee, volunteer, or trainee, performs an activity involving the use or disclosure of individually identifiable health information. These activities include claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, repricing, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. (Condensed from 45 CFR 160.103)
- f. **Minimum Necessary** - When using or disclosing PHI or when requesting PHI from another covered entity, a covered entity must make reasonable efforts to limit PHI to the

minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

- g. **Treatment** - The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.
- h. **Payment** - The activities undertaken by PHD to obtain or provide reimbursement for the provision of health care billing, claims management and collections activities.
- i. **Operations** - Activities that are related to covered functions, including conducting quality assessment and improvement activities, outcomes evaluation and development of clinical guidelines, population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contracting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment.
- j. **Employee Access to PHI** - Daily activities necessitate access to PHI for certain job descriptions. The following job descriptions are entitled to access PHI for TPO purposes:
 - Nurse Practitioner, MD, RN, LPN, Clinical Assistant, HHA, SWS, Dietician, PT, OT, ST and Students (nursing, medical, nutrition or PA) that are doing a rotation at PHD;
 - WIC staff may access the immunization portion of PHI for WIC clients;
 - Environmental Health staff may access PHI associated with reportable disease investigations; and
 - Clerical staff may access the minimum necessary portion of the PHI that is required for billing, making appointments, filing and other duties as assigned.
- k. **Authorized Access or Disclosure** - Access or disclosure of Protected Health Information that is necessary to support treatment, payment or business operations when authorized by the patient or as otherwise permitted by law.
- l. **Violation** - Access, use, or disclosure of PHI for purposes other than those for which the individual is authorized. See 1-5A.

2. **HIPAA Training Requirements and Privacy Officer**

All PHD employees will be trained upon employment, and at a minimum of every two years with updates as needed, to assure understanding of PHD's privacy procedures. Employees will access training at HIPAAtraining.com to successfully complete the training. Training dates and certificates of training are maintained in PHD's HIPAAtraining.com account online.

PHD's HIPAA Privacy Officer is responsible, under the direction of the Director, for compliance with the HIPAA Privacy Rule. PHD is served by outside legal counsel who may also provide HIPAA advice.

Protocol 1-5B: HIPAA Information and Procedure Manual

The [HIPAA Information and Procedure Manual](#) is a collection of required HIPAA forms and procedures to be used for informing patients of their privacy rights, obtaining authorization to release records, requests for access to records, patient privacy complaints, etc. The Manual is located on SharePoint/District Policies and Procedures/HIPAA.

Protocol 1-5C: HIPAA Training and Testing

Staff will complete HIPAA online training, testing and certification via [HIPAATraining.com](#) within 30 days of employment and every two years thereafter. HIPAA related reminders will be disseminated to staff via email and through Executive Staff meeting minutes as determined by the HIPAA Privacy and Security officers.

Protocol 1-5D: Confidentiality

The District Director, pursuant to powers and duties described in [Idaho Code 39-413](#), prescribes the following:

1. Confidentiality pertaining to PHD clients and/or patients should be maintained at all times.
2. Protected Health Information (PHI) is confidential and subject to HIPAA regulation. PHI is not open to the public or unauthorized District personnel.
3. Unauthorized possession, use, copying or reading of any PHD documents, client or employee records or disclosure of information contained in such records by or to unauthorized persons is prohibited.
4. No employee shall breach confidentiality by discussing information regarding a client by name or in a way by which the client can be identified or by discussing matters involving another District employee unless such information is necessary to render service provided by the District. Patients/clients must be assured that the information they provide will be protected.
5. Some patients/clients may not want their visit to PHD revealed, therefore, all PHD employees shall refrain from acknowledging patients in the clinic they know if at all possible. A patient visit to a PHD clinic is considered private and patient privacy rights are to be considered at all times. In addition to information contained in official records or patient charts, all other written, spoken, or visual information concerning any patient or client is confidential and must be protected accordingly.
6. All complaints alleging breaches of confidentiality will be investigated in accordance with PHD's HIPAA procedure found in the [HIPAA Information and Procedure Manual](#) and documented on the [Customer Service Satisfaction](#) form. A breach of confidentiality violation is grounds for disciplinary action up to and including termination of employment.
7. In the event that an employee, volunteer, student or Home Health contractor becomes aware that they have revealed a confidence, they will notify their supervisor immediately. If

the appropriate supervisor is unavailable, the incident should be reported to the District Director immediately and as soon as possible thereafter to the supervisor.

Protocol 1-5E: Requests for and Release of Protected Health Information (PHI)

PHD may receive a request for a patient's PHI from another covered entity. The appropriate Division Administrator or supervisor will determine if the information being requested is considered confidential and may, as required, with other appropriate staff or legal counsel, to either approve or deny a request for disclosure. In the absence of the Division Administrator, the District Director will act for him/her.

When such a request is received, the procedures below for each method of releasing information shall be adhered to before revealing PHI. No matter how insistent the requestor is, information CANNOT be disclosed about a patient before following the procedure that applies to the purpose of the request. Unauthorized disclosures are subject to disciplinary action. All disclosures will take place at District offices during regular office hours and in accordance with HIPAA regulations.

1. Request for Treatment, Payment or Operations (TPO) Purposes

Requests related to TPO may be made via telephone, fax, letter, electronic means or in person. In all cases, **first** determine if the request is for treatment, payment, or health care operations purposes (TPO). If the request is made solely for TPO and the requestor is not a "known requestor", request a fax on their official letterhead.

2. Patient Authorization to Use or Disclose Protected Health Information (PHI)

All PHI not related to TPO is not subject to public disclosure because of the confidential nature of the PHI. If a request is for other than TPO purposes, the request must include an authorization from the patient to release the information to the requesting party. The ***Authorization for Release of Information*** form is available in the [HIPAA Information and Procedure Manual](#). This form must be completed in its entirety by the patient/client. The request shall be filed in the patient record.

Prior to releasing any information for other than TPO purposes, contact the Privacy Officer or the Division Administrator. If uncertain as to how the information will be used, contact the Privacy Officer for clarification.

3. Subpoena

Follow the procedures in District [Policy 1-13 Information Release and Handling of Subpoenas](#).

4. In-Person Request

If an individual comes into the office and makes an in-person request to view or obtain copies of their own PHI:

- a. First verify the identity of the individual using a picture ID. Make a copy of the identification.
- b. Have the requestor fill out and sign the **In-Person Request for Access to Patient's Health Information** (located in the [HIPAA Information and Procedure Manual](#)).

5. Over the Phone or Electronic Requests

If an individual calls and requests PHI from their own record, verify the identity of the caller by asking for their name, address, birthdate, and social security number. If they are requesting PHI for a minor or they are a legal guardian ask for the client's name, address, birth date, and social security number. Check the client's medical record to verify the caller's relationship with the client, paying particular attention to whether the client is a minor and the caller has legal right to access the client's PHI. Document the call in the medical record with the caller's information and PHI requested. If the request is electronic, PHD personnel must contact the requester by telephone and follow the above steps.

6. When a Release Authorization is Not Required

[45 CFR 164.512](#) provides that the release of PHI without an authorization for the purpose of reporting abuse, neglect or domestic violence requires that the victim be promptly informed that the report has been or will be made, except: If the District, in the exercise of professional judgment, believes informing the victim would place the victim at risk of serious harm; or if the District would be informing the personal representative and the District reasonably believes that the personal representative is responsible for the abuse or neglect and that informing the personal representative would not be in the best interest of the victim. Information, either obtained directly for providing medical care or obtained incidental to the provision of care, which indicates elder/child abuse or that the child/elder has been sexually abused must be reported in accordance with [Idaho Code 16-1619](#) and [Idaho Code 39-5303](#) per Panhandle Health District's [Abuse Policy 1-22](#). In such cases, a release is not required.

Protocol 1-5F: Sanctions on Violations

1. Unauthorized individuals who access, use, and/or disclose PHI, attempt to access PHI, and/or assist others to access PHI when it is not authorized, will be sanctioned appropriately. As outlined in this protocol, a sanction may take the form of verbal counseling, written warning, or disciplinary action, up to and including termination.
 - a. **Level 1:** An employee **carelessly** accesses PHI that they have no need to know in order to carry out their job responsibilities, or carelessly reveals information to which they have authorized access. Examples of Level 1 violations include, but are not limited to:
 - Leaving PHI in a public area;
 - Misdirecting faxes or emails that contain PHI;
 - Discussing PHI that the employee is authorized to have accessed in public areas where the discussion could be overheard;
 - Leaving a computer accessible and unattended with PHI unsecured.
 - b. **Level 2:** An employee **intentionally** accesses PHI without authorization. A Level 2 violation shall be considered serious misconduct. Examples of Level 2 violations include, but are not limited, to:
 - Intentional, unauthorized access to a friend's, relative's, co-worker's, or any other individual's PHI (including searching for an address or phone number);
 - Intentionally assisting another employee in gaining unauthorized access to PHI;
 - Intentional, unauthorized access to Human Resource records or employee health files.

- c. **Level 3:** An employee **intentionally accesses and discloses** PHI without authorization. A Level 3 violation is considered serious misconduct. Examples of Level 3 violations include, but are not limited to:
- Unauthorized intentional disclosure of a friend's, relative's, co-worker's, public personality's, or any other individual's PHI;
 - Unauthorized delivery of any PHI to any third party.

2. **Procedures**

Each employee must report all alleged, apparent, or potential violations of confidentiality promptly (within no more than 24 hours) to their supervisor/designee. Any report of a violation of confidentiality shall be investigated in accordance with [Customer Service Policy 1-3](#). Upon receiving report of a possible HIPAA violation, the HIPAA Privacy Officer and Human Resources Specialist will be part of the investigation as well as the Division Administrator.

The Division Administrator is responsible for recommending the appropriate sanctions to the District Director. The investigation and decision will be documented in writing and maintained electronically by Administration. The District Director retains final authority concerning sanctions and will authorize any sanction involving suspension, dismissal, or termination before it is implemented.

The HIPAA Privacy Officer shall provide an annual report of all breaches of confidentiality to the District Director at the beginning of each calendar year.

The following will serve as guidelines for appropriate sanctions in circumstances where it has been determined that HIPAA and/or PHD privacy policies have been violated:

a. **Employees and Volunteers**

- Level 1 Violations shall result in verbal counseling which will be documented, and/or retraining. Multiple careless unintentional Level 1 Violations shall be subject to progressive disciplinary action up to and including termination. Retraining shall be required.
- Level 2 Violations shall result in a Notice of Contemplated Action with a three to five-day suspension, without pay in most instances, for the first Level 2 Violation. Retraining shall be required. Disciplinary action up to and including termination may be taken for multiple Level 2 Violations or when access was obtained under false pretenses.
- Level 3 Violations, in most cases, shall result in termination of employment or volunteer assignment.

b. **Vendors**

- Level 1 Violations may result in a verbal warning; written correspondence regarding the violation; and/or a request that vendor representatives be certified that they have retrained for HIPAA privacy.

- Level 2 Violations may result in written correspondence regarding the violation; a request that vendor representatives be certified that they have retrained for HIPAA privacy; a request that the company assign a new representative(s) to conduct its business with the institution; and/or suspension of activity with the business associate for a period of time to be determined.
- Level 3 Violations may result in written correspondence regarding the violation; a request that the company assign a new representative(s) to conduct its business with the institution; suspension of activity with the vendor for a period of time to be determined; and/or termination of the relationship with the vendor.

Corrective action for violations of confidentiality involving vendors shall involve the Financial Officer and shall include review of the vendor's contract.

Protocol 1-5G: Electronic Protected Health Information (ePHI) Procedure - Access, Storage and Security

This Protocol establishes standards to prevent, detect, contain or correct HIPAA security violations; and protect information stored on workstation computers, laptops, mobile devices and network infrastructure that are authorized to operate within Panhandle Health District. Since data that is created, manipulated and stored on these systems needs to be protected, it is essential that the computer systems and the computer network, as well as the data they store and process, be operated and maintained in a secure environment and in a responsible manner. It is also critical that these systems and machines be protected from misuse and unauthorized access and those users follow the acceptable use policy. ([Computer, Telephone and Information Systems Acceptable Use Policy 5-1](#))

Section I - Risk Management

1. Risk Analysis

Executive Staff, with input from the Information Technology (IT) staff, will define the purpose and function of PHD's electronic resources and establish acceptable levels of security risk for resources by assessing factors such as the sensitivity of the data and whether or not the information is protected by law or policy. The HIPAA Privacy and Security Officers, in conjunction with IT, will perform Risk Analysis annually and when the ePHI security environment changes.

2. Risk Assessment/Management Methodology

The following methods will be used for risk management:

- a. Identify, characterize and assess threats.
- b. Assess the vulnerability of critical assets to specific threats.
- c. Determine the risk (i.e. the expected likelihood and consequences of specific types of attacks on specific assets).
- d. Identify ways to reduce those risks.

- e. Prioritize risk reduction measures based on current best-practices/industry standards.

Section II – Technical/Non-Technical Evaluation

1. Evaluation Standard

PHD will conduct a thorough technical and non-technical evaluation of security controls and processes periodically, but not less than every five years, or when environmental or operational changes occur that significantly impact the confidentiality, integrity or availability of its ePHI. Such changes include but are not limited to:

- a. Significant security incidents to PHD information systems.
- b. Significant new threats or risks to PHD information systems.
- c. Significant changes to the organizational or technical infrastructure of PHD.
- d. Significant rule changes to information security requirements or responsibilities.

Such evaluations should at a minimum include:

- a. A detailed review of PHD security policies, procedures and standards to determine whether they are still effective and appropriate.
- b. Identification of the risks to PHD information systems if environmental or operational changes occur
- c. Carried out only by authorized and appropriately trained persons (may include contractor personnel).

The results of all such evaluations must be formally documented and reviewed by the Executive team. The document will reside in a secure portion of the network with limited access to only those whom have a need-to-know.

2. Business Associate Contracts and Other Written Agreements

PHD may permit a business associate to "create, receive, maintain or transmit" electronic protected health information (ePHI) on its behalf. However, it may do so only if there are "satisfactory assurances" that the business associate will appropriately safeguard the ePHI. Written agreements documenting such assurances are required for any Business Associate relationship.

3. Implementation Specifications: Written Contract or Other Written Agreements

The contract or other written agreement must provide that a business associate will:

- a. Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic PHI that the business associate creates, receives, maintains, or transmits on behalf of the covered entity;
- b. Ensure that any agent, including a subcontractor, to whom the business associate provides such information agrees to implement reasonable and appropriate safeguards to protect it;
- c. Report to the covered entity any security incident of which it becomes aware; and,

- d. Authorize termination of the contract (or other arrangement) if the covered entity determines that the business associate has violated a material provision.

Section III – Security Standards

1. Security Responsibility

PHD has designated the IT Program Manager as the HIPAA Security Officer who will be responsible for maintaining and assuring that staff are properly trained on the District's HIPAA policies and procedures to include a testing process to assess comprehension.

2. Workforce Security

- a. Applications must be designed, and computers must be used in a manner that will protect the privacy and confidentiality of the various types of electronic data being processed, in accordance with applicable laws (HIPAA, HITECH Act) and District policies.
- b. Users who are authorized to obtain data must ensure that it is protected to the extent required by law or policy. For example, when sensitive data is transferred from a well-secured server system to a user's location, adequate security measures must be in place at the destination computer to protect this "downstream data". PHI must not be stored on destination device (e.g. C: drives). Exceptions may be granted by the HIPAA Security Officer with sufficient encryption protocols in place and concurrence by the HIPAA Privacy Officer.
- c. Technical staff assigned to ensure the proper functioning and security of district electronic information resources and services are not permitted to search the contents of electronic communications or related transactional information except as provided for by guidance from the IT Manager or the Environmental & Health Protection Division Administrator in his/her role as Division Administrator of IT.

3. Authorization/Supervision

- a. Unique user identification (user ID) and authentication is required for all systems that maintain or access the domain. Users will be held accountable for all actions performed on the system with their user ID. District password procedures and protocols will be used at all times.
- b. Management authority for each electronic medical records (EMR) software program will be designated by the Public Health Services (PHS) Division Administrator. The Clinical Services Nurse Manager will maintain a list of staff who are authorized to have access to the EMR system. The Nurse Manager and PHS Division Administrator will authorize access for new employees and direct changes in access if assigned duties are changed. The Nurse Manager will review this access authorization list with the HIPAA Security Officer semiannually.
- c. The PHS Division Administrator will maintain a list of staff who are allowed access to web-based sites that contain ePHI. This list will be reviewed semiannually to ensure access is appropriate.

- d. Supervisors will define network access rights for each user when they are hired or change positions. Supervisors will complete the back side of the Job Announcement Form (JAF) to indicate the level of network access authorization for new employees and Division Administrators will review and approve access levels.
- e. After a vacant position is filled, and approved by the District Director, the HR Specialist will complete the SharePoint New Employee Form and which alerts IT staff for network setup.
- f. Additions or modifications of network rights to ePHI will be sent by the employee's supervisor or the manager who has responsibility for that area of the network to which the access is to be granted and approved by the appropriate Division Administrator. The request should be submitted via an online service ticket to IT at least 24 hours prior to rights modification.
- g. The Nurse Manager for Clinical Services and the Program Manager for Epi/Health Promotion will control who has access to the network P/FACH drive where ePHI can be stored. These two managers will maintain the list of authorized users and review that list with the HIPAA Security Officer semiannually. Additionally, these two managers, in conjunction with the IT staff will audit their authorization list with actual network permissions and resolve any differences.

4. Employee Separation/Dismissal Procedures

- a. The HR Specialist will notify IT immediately in the event of an employee separation, dismissal or placement of an employee on administrative leave. Additionally, the HR Specialist will ensure that physical keys and other access devices are secured. In the event keys/codes are not secured/returned, the HR Specialist will consult with HIPAA Security Officer for rekeying/re-coding of locks.
- b. The IT staff will immediately disable the user account(s) and disable any remote access the employee may have had. Employee building access badges will be terminated as well.
- c. The HR Specialist will notify IT staff if that employee's phone or e-mail is to be forwarded to another employee or supervisor.
- d. The employee's supervisor will notify IT staff of the final disposition of the employee and provide guidance as to archiving of the employee's data. The supervisor will also inform IT staff if the employee account should be deleted or be transferred to a new employee. The disposition of the employee's phone services and greetings for that number should also be provided. The HR Specialist will inform IT when an employee's access is to be disabled immediately under circumstances such as dismissal or other disciplinary action. IT will in turn secure all electronic media/devices associated with that employee for review by the HIPAA Security Officer.
- e. For staff who had access to one of the EMR systems, the EMR manager will take action to get that access removed and so document on their access list.
- f. If no notice is given to IT staff, disabled accounts will be deleted 180 days after termination or separation. Exceptions will exist for cases of ongoing investigations or legal actions.

5. Access Authorization

In addition to the Authorization/Supervision requirement in Section III.3.a, users must adhere to the following security procedures:

- a. Secure the user's authentication control (e.g. password, token) that it is known only to that user in accordance with PHD password security procedures. Passwords will not be written and/or stored in any form of media without adhering to PHD approved storage procedures/systems.
- b. Log off, lock or setup a password-protected screensaver when leaving the workstation unattended.
- c. The local administrator account must be password protected in accordance with PHD password procedures.
- d. PHD will not utilize guest accounts without specific written approval of the HIPAA Security Officer.
- e. PHD will utilize a lockout policy that limits users to three attempts and an automatic reset after 30 minutes.

6. Security Reminders

- a. The HIPAA Security Officer will ensure that IT sends reminders of good security practices via email on an as needed basis but not less than semi-annually.
- b. IT will publish security alerts, vulnerability notices and patches, and other pertinent information in an effort to prevent security breaches. Exchange archiving will track alerts and be retained for a minimum of three years.

7. Malicious Software Protection

All server, workstations and other devices will have anti-virus software installed and operating whether on the PHD network or not.

8. Logging and Monitoring

PHD may employ logging and monitoring management software for network activity.

9. Password Management

All PHD employees shall maintain a password with the following characteristics:

- a. Minimum of 16 characters, which includes spaces. Passphrases are recommended.
- b. Passwords will be changed if compromised or assessed vulnerable. Vulnerability assessments will be conducted periodically by IT under HIPAA Security Officer review.
- c. Password policy will be enforced by IT procedures and reviewed by HIPAA Security Officer annually.
- d. No user shall share their password with anyone.
- e. The local administrator account will be secured in accordance with 5c. above.

10. Information System Activity Review

- a. IT staff will maintain network management software that will notify them of potential security issues.
- b. Settings of the network management software will enable logging and auditing at the operating system, network appliance and application/database levels. Review of the following will be conducted as appropriate for the device/system.
 - 1) Failed and successful logins
 - 2) Modification of security settings
 - 3) Privileged use or escalation of privileges
 - 4) System events
 - 5) Modification of system-level objects
 - 6) Session activity
 - 7) Account management activities including password changes (success and failure)
 - 8) Policy change
 - 9) Network firewalls
 - 10) Removal of or shutdown of anti-virus/anti-malware products
 - 11) Application installation such as web servers
- c. The following information should be captured for each of the above items as appropriate:
 - 1) Date and time of activity
 - 2) For connection logs: peer IP address
 - 3) Identification of user performing activity
 - 4) Description of attempted or completed activity
- d. The IT Manager is responsible for defining and ensuring appropriate logging/monitoring. The log monitoring software will be set to notify all IT staff by email for all identified security problems. The email archiving process will allow retrieval of the notifications.
- e. IT staff will escalate security-related issues, questions or concerns to IT.
- f. On a quarterly basis, IT will audit all security problem notifications and document his findings to the HIPAA Security Officer.

11. Facility Security

Appropriate controls must be employed to protect physical access to resources commensurate with the identified level of acceptable risk. These controls may range in scope and complexity from extensive security installations to protect a room or facility where server machines are located, to simple measures taken to protect a user's display screen. The following controls will be adhered to:

- a. Staff will position screens in a manner that external customers cannot view.
- b. The Division Administrators will determine which doors will be unlocked during business hours.
- c. Office areas will be locked whenever they are not occupied.
- d. Doors to areas that cannot readily be monitored will be secured.

- e. All employees will wear their ID Badges whenever they are on district property to aid in identifying unauthorized individuals.
- f. Enhanced measures of building access will be employed with a balance of security and business necessity.
- g. Building security systems, including video monitoring equipment will be reviewed by the HIPAA Security Officer to ensure that these systems do not conflict with ePHI protections. Access to video images will be limited to essential personnel and approved by the District Director.

12. Facility Access Controls

Access cards and codes to enter buildings will only be distributed to authorized personnel and must be approved prior to release. Cards and access groups will be defined and approved by the Division Administrators and District Director. The HR Specialist will notify IT staff of any revocation/changes in access. The HR Specialist will control all keys to physical locations.

13. Facility Maintenance Records

PHD shall implement maintenance procedures that require documentation of repairs and modifications to physical components of a facility which are related to security (i.e. server room doors and locks). Documentation shall include the repair, addition, or removal of devices utilized in providing physical safeguards of secured Information Technology facilities. The HIPAA Security Officer will review all security related repairs/maintenance etc. The HR Specialist will coordinate with the HIPAA Security Officer on these actions. Changes will be e-mailed to IT for storage in SharePoint: IT Documents/Physical Security Changes Server Room folder.

14. Workstation Security Standard

- a. Workstations and other connected devices will be password protected in accordance with 9. above. PHD employees shall logout when away from their devices. Automatic logout will also be defaulted to all PHD devices. Additional protections such as privacy screen covers/filters and positioning of screens away from public view (including windows) will be employed as necessary and determined by the HIPAA Security Officer and Division Administrator.
- c. Passwords will not be shared.
- d. When workstations are removed from service the machine will be thoroughly wiped to ensure no ePHI remains. The HIPAA Security Officer will periodically review IT cleansing procedures to ensure they are compliant.
- e. Thumb drives will not be utilized to download or store ePHI.

15. Audit Controls

- a. System and data owners are required to proactively and reactively engage audit processes to detect unauthorized access attempts. Reactive audits are performed whenever a defined event triggers the need for an audit. An "event" might be a patient complaint or a security systems alarm.
- b. It is also advisable to audit appropriate logs when unusual or extreme situations occur.

- c. When an involuntary termination of an employee occurs, all systems containing PHI must be monitored for potentially malicious activity.

Section IV - Security Incident Procedures

1. Implementation Specification: Response and Reporting

- a. Virus Incidents: IT will immediately disconnect any computer affected by a virus unless the virus is quarantined by the Anti-Virus software, until verified that the threat is eliminated.
- b. Log Review Anomaly: Suspicious entries in Event Log Management Software will be identified and validated as an actual threat or false alarm. Login failure incidents will be validated by contacting the user to confirm they had an issue. If it is unclear that they had logon failures, the user's password must be changed immediately, either by the user or the Network Administrator.
- c. If a breach occurs, all involved personnel will apply due diligence in retaining any information regarding the attack for investigation.
- d. Containment will be prioritized based on the threat. A PC or server may be disconnected from the network if it is a threat. If IT becomes aware of a threat currently in process, that WAN connection may be suspended until the threat is cleared.
- e. Reporting Violations and Potential Breaches: All PHD staff, volunteers and contractors must immediately report privacy violations or loss of ePHI, such as the loss or theft of a computer, smartphone, or any electronic intrusion into a computer storing ePHI. Reports will be made to the HIPAA Security Officer, who will also consult with the HIPAA Privacy Officer.

Section V – Preventing Data Loss

1. Data Backup Plan

- a. The IT Data Backup Plan defines the backup for computer systems that store PHD data and is designed to prevent the loss of PHD's data in the event of an equipment failure or destruction. Backup data is stored separately from the original on different storage media or additional hardware used to restore the original in the event of a data loss.
- b. The backup systems are typically servers but are not necessarily limited to servers. PHD's servers that are backed up include the File server, Web server, SharePoint server, TEC Storage server and database server. Emails are stored in the cloud and are archived outside of PHD's network.
- c. The backup guidelines below apply to all servers maintained by PHD, but does not apply to PC workstations, laptops and applicable peripherals that do not store original or source documents and data for the District.

2. IT Staff Backup Strategy Guidelines

- a. Identify computerized systems that store source or original PHD information.
- b. Standard frequency and type of backup for each type of computer system or platform is defined in the [PHD Backup Procedure guide](#).
- c. The backup is tested semiannually to determine if data files and programs can be recovered.

3. User Responsibilities

- a. Each user will store their data on approved network drives.
- b. Each group of users will have different drives to store data based on their section and position. All users will be provided with a “Home Directory” (H-Drive) to store their work.
- c. All scan-to-folders and folders designated as “Temporary Files” will not be backed up.
- d. Data storage on a user’s personal workstation, i.e. the “My Documents” folder or the local “C” Drive will not be backed up.
- e. All PHD laptops and mobile devices that are utilized to access EMR systems shall be encrypted.

4. Data Integrity/Integrity Controls

- a. Only properly authorized and trained PHD staff may access and use ePHI on PHD IT information systems. Methods used to protect the integrity of ePHI contained on PHD information systems must ensure that the value and state of the ePHI is maintained and protected from unauthorized modification and destruction.
Data is authenticated by using industry best practices or industry standards.

5. Data Restoration

- a. Employees may request a restoration of lost or damaged files as well as previous versions of files using the IT Help Desk Ticket on SharePoint.
- b. Users will provide IT with the location of the file, file name, reason for restoration and date/version of the file in question. IT will restore the file if it is available and possible.

6. Backup Schedule and Details

- a. The SQL database is backed up twice daily to the default SQL server located at the Hayden PHD Office, at noon and at 6:00 p.m. local time. Backups are then transferred to the Storage Area Network (SAN – a Disk-to-Disk (D2D) that evening and eventually off loaded to tape when full Disk-to-Disk-to-Tape (D2D2T) backups are complete.
- b. Major files such as in the “P” drive, user folders, database files, TEC scans, etc. are replicated to Sandpoint’s SAN unit every evening in case of a catastrophic event at the Hayden office.
- c. TEC scans and the TEC database files are transferred weekly to PHD’s demilitarized zone (DMZ) so there is public access to septic and food data on PHD’s public website, and therefore, another backup of the TEC Environmental system is achieved.
- d. An incremental backup is performed every Monday through Thursday onto a SAN-Disk and stored until the disk overwrites. The data is available for one week. A full backup is performed every Friday onto a SAN-Disk.
- e. A full backup is performed every Monday via Trans to Tape and stored for four weeks. It is stored in the server room and the previous backup tape is transferred to the safe for two weeks. The older backup tape from the safe is taken off-site.

7. Backup Retention

- a. At least three different backup copies are available at all times, one of which is physically stored in a different location from the others. The “off-site” backup is never older than one month.
- b. Additionally, depending on the nature of the data, one medium (tape or portable hard drive, etc.) is designated as a monthly backup and kept for at least three months.
- c. A year-end backup on a portable storage device capable of storing all data sets is kept offsite.
- d. Backup tapes not kept in the locked and monitored server room, are stored in the IT tape safe in the Fiscal records fire-resistant room.
- e. The offsite tape rotation is maintained in a PHD supplied safe at the IT Network Analyst’s residence.
- f. A SQL Manager Software backs-up SQL data at noon and 5:00 p.m. local time as a precautionary backup in case of data corruption.

Section VI - Disaster Recovery/Emergency Operations

1. Disaster Recovery Plan

See the [Continuity of Operations Plan, Annex C3](#)

2. Power

- a. Backup generator power systems and/or Uninterruptible Power Supplies (UPS) shall be managed and network-connected to protect routers, LAN switches and VoIP systems.
- b. UPS systems should include Ethernet-based network management cards capable of Simple Network Management Protocol (SNMP) monitoring via TCP/IP.
- c. Power management systems will be automatically tested weekly.

3. Emergency Restoration/Operation

- a. PHD’s emergency response vehicle (ERV) has stand-alone (generator power and satellite) internet capability which would allow PHD personnel to access cloud-based functions such as email, etc. Limited functions would be available to operate as defined in the Continuity of Operations plan (COOP).
- b. Limited wireless access for notebooks/tablets is available to connect to the ERV network as replacement workstations. Internet access will be available in most areas via the MiFi or satellite links to allow connection to web-based programs.
- c. The ERV also has an independent power generator capable of running network systems and a UPS device will be used for line conditioning.
- d. In response to an emergency where servers are destroyed, a new server would be purchased and put in the most secure and reliable location. Data would be restored as described in the Data Backup Plan (Section V.1.).
- e. The ERV would provide limited operational capability until location and equipment could be procured.

4. Testing and Revision Procedures

Testing and revision procedures are necessary to ensure contingency operations. The COOP will be maintained and exercised/tested at least annually to ensure PHD has the capability to continue operations.

5. Applications and Data Criticality Analysis

The IT Manager will establish criteria for assessing the relative importance of vulnerabilities and threats as part of the risk analysis and should prioritize steps in data backup, disaster recovery, and emergency mode operations. Applications and Data will be identified and categorized and implemented into plans for recovery of operations and safeguarding PHD's electronic systems and ePHI.

6. Contingency Operations

See the [Continuity of Operations Plan, Annex C3](#)

7. Emergency Access Procedure

- a. All PHD employees with remote access to email and SharePoint privileges are responsible to ensure that unauthorized users are not allowed access to internal PHD networks and associated content. VPN will be the sole method for accessing network drives and SharePoint.

Section VII - ePHI Data on Portable Devices

1. Smartphones and Other Mobile Data Devices

PHD personnel should take reasonable steps to secure their issued mobile devices. A PHD mobile device should NOT be stored in a vehicle, whether staff is at a client's house, home overnight or any other activity, even if the vehicle is located in the PHD parking lot. Portable devices are vulnerable to theft, especially when in plain view within a vehicle. All mobile devices will employ password protection methods approved by PHD's IT Manager. Other than pre-approved devices and systems that access web-based applications, mobile devices will not be used to store ePHI of any kind without the express written approval of the HIPAA Privacy and Security Officers.

The loss of a mobile device must be reported to IT staff immediately, so it can be remotely wiped. If the loss occurs after hours, employees will contact their supervisors who will, in turn, contact IT staff to take necessary actions. This must be done as soon as a device is determined to be missing or unaccounted for.

2. Removable Media Devices

No ePHI files will be downloaded or stored on a thumb drive or similar removable storage device.

3. File Transfer

- a. No email transmission of ePHI is allowed to leave the PHD1 domain.
- b. Email sent from the PHD1 domain to a receiver also on the PHD1 domain is secure within the domain, however it is not encrypted. Therefore, care must be taken to ensure ePHI is not subject to unauthorized disclosure. Do not use public Wi-Fi connections to transmit PHD1 to PHD1 emails containing ePHI.

Section VIII – Disposal of Data

1. Data Sanitizing

All electronic media must be properly sanitized before it is transferred from the custody of PHD. The proper sanitization method depends on the type of media and the intended disposition of the media. Electronic media may be scheduled for reuse, repair, replacement, or removal from service for a variety of reasons and disposed of in various ways as described below. The IT Manager and the HIPAA Security Officer will periodically review sanitizing procedures to ensure they comply with industry standards and/or best business practices.

- a. Overwriting hard drives is an approved method of sanitizing a hard disk storage device. Overwriting of data means replacing previously stored data on a drive or disk with a random pattern of meaningless information. This effectively renders the data unrecoverable when correctly done.
- b. Destruction of electronic media is the process of physically damaging a medium so that it is not usable by any device that may normally be used to read electronic information on the medium.
- c. Disposal of Hard Drives - Prior to disposal, operable hard drives must be overwritten in accordance with the procedures in VIII.1.a above. Equipment designated for surplus or other disposal must have a label affixed stating that the hard drive has been properly sanitized per DOD-5220.22 standards.
- d. Disposal of Damaged Drives - IT staff must first attempt to overwrite the hard drive in accordance with the procedures in paragraph 1.a above. If the hard drive cannot be overwritten, the hard drive must be mechanically damaged so that it is not usable by a computer.

2. Media Re-use

- a. All electronic media must be properly sanitized before it is transferred from the custody of its current user.
- b. The proper sanitization method depends on the type of media and the intended disposition of the media.
- c. The disposal procedures used will depend upon the type and intended disposition of the media.

Protocol 1-5H: Accessibility and Authorization to Enter the Hayden PHD Building after Hours

1. The security alarm system is automatically activated (armed) every day at midnight until 6:00 a.m. the next morning, including weekends and holidays. Access badges for all staff other than those authorized in item 2, will only work during the non-alarmed times.
2. Only staff designated by the Director and Division Administrators are authorized to enter the building between midnight and 6:00 a.m. Authorized staff include:

District Director
Public Health Services Division Administrator
Environmental and Health Protection Division Administrator
Fiscal Officer
Facilities Maintenance Manger
Human Resources
Management Assistant
Public Health Preparedness Program Manager
Environmental Health Program Manager
Home Health Program Manager
Home Health Nurse Manager
Health Promotion Program Manager
Immunization Coordinator
IT Staff including Kootenai Health IT Staff with access badges
Child Care Resource Center (CCRC) Program Coordinator
3. Authorized staff must be trained by IT Manager and follow the steps outlined in the alarm/access procedures published under separate cover. Authorized staff will be issued a wallet sized card with these procedures.

Protocol 1-5I: Photography Video and Electronic Imaging or Recording

Because of the confidential nature of our client relationships and the importance of existing privacy laws and regulations, PHD restricts the use of photography, filming, video or any other form of electronic imaging or recording on and about its facilities.

Accordingly, the taking of photographs, video or any other form of electronic imaging or recording of PHD facilities, staff, clients or security and surveillance systems is expressly prohibited unless authorized in writing by the Director of PHD or her/his designated representative. This includes recording the physical buildings and grounds, PHD's offices and other facilities, including temporary facilities established to provide services to the public that are not already fixed/permanent existing PHD facilities.

This protocol includes all public access areas of PHD facilities, as well as clients and their activities in these public areas. This is necessary to protect their rights under HIPAA and other laws and regulations applicable to PHD.

1. Anyone desiring to take photographs, video or any other form of electronic imaging or recording on PHD grounds must obtain prior written permission from the Director, PHD or her/his designated representative. A ***Request to Photograph, Video or Record***, will include the requestor's name, address and contact information, as well as proof of identification (government issued drivers license or identification card) and will clearly articulate the reasons necessary for photography, video or any other form of electronic imaging or recording.
2. Officially sanctioned photography, video and other electronic imaging or recording, which is approved through PHD PIO is allowed, provided all other provisions of PHD policy and protocols, as well as applicable laws and regulations are met. This includes PIO directed media events, etc. A ***Media Release Form***, must be completed for each person imaged, including employees, agents, clients or others. Such sanctioned recording activity shall not image PHI or PII, nor shall it image any security systems or activity.
3. This protocol is not intended to prevent photographs or video taken by PHD staff at occasional events, where clients and the public are not receiving direct PHD service, such as staff recognitions or celebrations. This protocol does not prohibit law enforcement officers or other investigators authorized by law from taking photographs, video or other electronic imaging or recording in accordance with their official duties.
4. Violations of this protocol may result in the individual being trespassed from PHD facilities and may result in other civil and criminal action.

Notwithstanding the above, video and/or audio recording will be allowed by the public and media during Board of Health meetings conducted pursuant to the Open Meeting Act, when in open session, as long as the recording is unobtrusive and does not create a distraction or interfere with the Board meeting.



Public Health
Prevent. Promote. Protect.
Panhandle Health District

Panhandle Health District

Healthy People in Healthy Communities



Request to Photograph, Video or Record

I am requesting permission to take photographs, video or record some form of electronic image on or in Panhandle Health District (PHD) property.

Date and time of Photography, Video or Recording: _____

The purpose of my request is:

Printed Name: _____

Address:

Street _____

City _____ **State:** _____ **Zip**

Code: _____

Phone: _____

ID/DL Number: _____ **State/Jurisdiction:** _____

I certify (or declare) under penalty of perjury pursuant to the law of the State of Idaho that the foregoing is true and correct.

(Date)

(Signature)

I understand that, if approved, I may only take photographs or video/record images specifically approved by PHD. Failure to comply with the conditions placed by PHD will result in the revocation of permission and may result in a trespass order or other civil and criminal action.

Approved: _____ **Disapproved:** _____

(Panhandle Health District)

(Date)

Conditions of Approval:



Public Health
Prevent. Promote. Protect.
Panhandle Health District

Panhandle Health District

Healthy People in Healthy Communities



Media Release Form

I understand that services provided by Panhandle Health District may include medical procedures and that my health care information is protected under Idaho Code 9-340C(13). I authorize Panhandle Health District to broadcast or publish any videotape/photographs and/or interview/testimonial taken of me during these procedures and special events, and that Panhandle Health District may use these videos/photographs and/or interview/testimonial of me on its social media sites, website, publications or newspaper articles. I understand that I will not be compensated for the use of my information, photograph/video or quote.

My initials below indicate that I authorize Panhandle Health District to use and/or disclose the following information about me:

_____ All photographs, videos, quotes/interviews of me may be used indefinitely unless I revoke this release

_____ My name

_____ My age, city, county and state of residence

Signature _____ Date _____

(If subject is a minor child under the age of 18, a parent or guardian must sign)

Printed Name _____

I understand that I may refuse to sign this authorization and that my refusal to sign will not affect my ability to obtain treatment or my eligibility for services.

Finally, I understand that I may revoke this authorization at any time, provided that I do so in writing. I understand that information released between the effective date of this authorization and the date of the revocation may still be used in the public domain.

Additional Information

1. Name of person/people featured: _____
2. Location: _____
3. Description of photo/media: _____
4. Name of staff member: _____
5. Other information you wish to provide: _____

