# OAKLAND COUNTYWIDE HIPAA PROCEDURES
Date Effective: 6/7/2018
Accountable: HIPAA Privacy Officer

# Table of Contents

# Introduction

The procedures listed in this document outline measures Oakland County will take to comply with HIPAA Privacy and Security Rules to ensure the security and privacy of protected health information (PHI) it maintains in operations as a hybrid entity.

# HIPAA Privacy Rule Procedures

## Section 1.01 Minimum Necessary Standard Procedure

### (a) Minimum Necessary Use and Disclosure Procedure

The following criteria should be considered in determining the minimum amount of information that must be released to carry out the intended purpose:

- type of PHI needed
- whether disclosure and use are to a person or class of persons who need access to the information to carry out their job duties relating to the Health Plan
- whether the use is for treatment, payment, or health care operations, or is made pursuant to a valid authorization by the individual, or otherwise allowed under HIPAA
- whether the task can be accomplished with less information
- whether, under the circumstances, the use or disclosure seems to be reasonably necessary and appropriate
- the risk that the use or disclosure will result in an unauthorized use or disclosure of the PHI
- if the disclosure will be to a third-party administrator or other service provider, whether the county has entered into a valid business associate agreement with that business associate
- whether the county has agreed to an additional restriction on the use or disclosure of PHI that would be violated by the use or disclosure

If the disclosure will be to a third party authorized to receive PHI, the county will use the same criteria as above, when applicable, to determine whether needed information is limited to the minimum necessary to accomplish the intended purposes. Examples of such third parties include:

- business associates
- other covered entities, such as an insurer with which the Health Plan coordinates benefits
- public officials or agencies for a permitted disclosure of PHI for legal or public policy purposes, such as the Department of Health & Human Services when it is auditing for HIPAA compliance

Minimum Necessary Standard Exceptions

The minimum necessary standard does not apply to:

- disclosures to a health care provider for treatment purposes
- disclosures to the individual who is the subject of the PHI
- uses or disclosures made pursuant to an authorization
- disclosures made to the Department of Health and Human Services (“HHS”)
- uses or disclosures in response to the order of a court or administrative tribunal (but such disclosures may not exceed the scope of the order)
- disclosures pursuant to process or as otherwise required by law (but only to the extent required by law)
- uses or disclosures that are required for compliance with the Privacy Rules

## Section 1.02 Notice of Privacy Practices Procedures

### (a) Notice Creation Procedure

The HIPAA Privacy Officer is responsible for developing and maintaining the Notice of Privacy Practices. The Privacy Officer also must ensure that the Notice complies with the requirements set forth in the Privacy Rules and that a copy of the Notice is maintained in accordance with the "Documentation and Record Retention Requirements Procedure."

## (b) Health Plan Participant Notice Delivery Procedure

The HIPAA Privacy Officer will ensure that Notice is delivered to participants in the Health Plan as follows:

- to each new enrollee in the Health Plan at the time of the individual's enrollment
- within 60 days of any material revision to the notice to individuals who are then covered by the Health Plan (unless HIPAA regulations allow for an alternative distribution schedule)

At least once every three years, the county will inform all participants then covered by the Health Plan that the Notice is available and how they can obtain a copy. The county will also provide a copy of the notice to any individual upon request. The county will document the delivery of the Notice in accordance with the "Documentation and Record Retention Requirements."

## (c) Delivery Notice to Patients Procedure

The Health and Human Services Department will ensure that Notice is delivered to the county's patients as follows:

- The county will deliver the Notice to each new patient on the date of the first treatment; or in an emergency treatment situation, the county will deliver the Notice as soon as reasonably practicable after the emergency treatment situation.
- Except in the case of an emergency, the county will make a good faith effort to obtain a written acknowledgment of receipt of the Notice in accordance with the Privacy Rules.
- The Practice will have the Notice available at its location(s) for individuals to request to take with them.
- The Practice will post the Notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the Practice's locations to be able to read the notice.

## (d) Electronic Delivery of Notice Procedure

Individuals may agree to receive the Notice by e-mail. The following rules apply to provision of the Notice by e-mail:

- if an individual agrees, the Notice may be delivered electronically by e-mail.
- an individual may withdraw permission to receive the Notice by e-mail at any time.
- if the county knows that an e-mail transmission to an individual has failed, the county must provide a paper copy of the Notice to the individual
- an individual who receives an electronic version of the Notice may request a paper copy at any time

## (e) County Website Posting Notice Procedure

If the county maintains a web site that provides information about employee benefits (including an intranet site with information on employee benefits, the Health Plan, etc.) or that provides information about its customer services, the county must prominently post the Notice on the web site and make the Notice available electronically through the web site.

## (f) Notice Revision Procedure

The county will revise the Notice whenever there is a change in law that requires a material revision to the Policies and Procedures, or whenever the county elects to make a material revision to the Policies and Procedures. When this occurs, the county will redistribute the Notice to Health Plan participants. To its patients, the county will make the

notice available upon request on or after the effective date of the revision and post the revised Notice in accordance with these Policies and Procedures.

## Section 1.03 Permitted Use for Payment and Health Plan Operations Procedures

### (a) Administration of Health Plan Procedure

HR Department benefits and/or retirement area employees have direct oversight responsibility for the county Health Plans and may use or disclose PHI for the purposes of administering the Health Plan. This includes all payment and health care operations permitted under the HIPAA Privacy Rule, including but not limited to the following activities:

- determining plan benefits and eligibility for benefits
- paying claims and providing benefits
- enrollment and disenrollment in benefit programs
- obtaining premium bids and quotes for administrative services, and other activities related to placement, renewal, or replacement of a contract of health insurance or for administration of health benefits (including stop-loss and excess loss insurance)
- determining costs of self-insured benefits and employee contribution amounts
- coordinating benefits with other plans and coverages
- final adjudication of appeals on claims appeals
- exercise of the Health Plan's rights of recovery, reimbursement, and subrogation
- obtaining employee contributions
- assisting participants and beneficiaries with questions relating to eligibility, benefits, appeals and other inquiries relating to the Health Plan
- evaluating plan performance and making recommendations to the county on plan design issues
- engaging in quality assessment activities
- complying with laws that apply to the Health Plan, such as, COBRA, Medicare Secondary Payer rules, etc.
- obtaining legal services relating to the administration of the Health Plan.
- performing auditing functions, including programs to detect fraud and abuse
- engaging in cost-management activities
- making claims under stop-loss or excess loss insurance
- engaging in business planning, management, and other general administration of the plan
- conducting activities relating to the transfer, merger, or consolidation of the Health Plan, including due diligence.

For these routine uses and disclosures, the HR department uses and discloses the minimum information reasonably necessary for the intended purposes under the Minimum Necessary Standard.

### (b) Health Plan Administration Change Procedure

Benefits and retirement administration activities are considered Health Plan records and are protected health information.

Qualified Medical Child Support Order

As a preliminary step toward the entry of a Qualified Medical Child Support Order (QMCSO), the county may receive a National Medical Support Notice (NMSN) or similar document that seeks information about one or more individuals covered under the county Health Plan. To the extent possible, HR Department employees will use only enrollment records to respond to such request.

## (c) Provision of Health Care Service Activities Procedure

The county may use and disclose an individual's PHI for treatment purposes and to perform the county's own payment activities or health care operations, as permitted under the Privacy Rules, including, but not limited to the following activities:

- provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party
- consultation between health care providers regarding a patient
- referral of a patient from the county to another health care provider
- billing and collection activities
- reviewing health care services for medical necessity, coverage, justification of charges and the like
- utilization review activities
- disclosures to consumer reporting agencies (limited to specified identifying information about the individual, their payment history, and identifying information about the Practice)
- engaging in quality assessment activities
- performing auditing functions, including programs to detect fraud and abuse
- engaging in cost-management activities
- engaging in business planning, management, and other general administration of the county, and
- activities relating to the transfer, merger, or consolidation of the health care services, including due diligence.

## (d) Use of Genetic Information Procedure

The HR department will not use any genetic information, including family medical history, to conduct eligibility determination or other underwriting activities relating to the Health Plan. This includes the computation of premiums or contribution amounts under the Health Plan.

## (e) Sharing PHI with Administrators Procedure

The HR department will use the administrator's secure transmission portals or other secure methods consistent with the Information Protection procedures in the HIPAA security section of these policies.

## (f) Claims Appeal Procedure

Although third party administrators typically handle the first level claims appeals, the HR department oversees the second level of the claims appeal process for the self-funded benefits offered through the Health Plan. This requires that HR department employees have access to PHI to the extent necessary to administer this appeal process.

The county will not be involved in the first level claims appeal process but will refer an individual who wishes to appeal an adverse benefit determination to the appropriate claims administrator, which will perform the initial review. If the first level appeal is denied and an individual chooses to pursue a second level appeal, the individual may submit the

appeal to the carrier who may refer it to an external appeal advisor. Any such advisors will be required to sign a business associate agreement in which they promise to protect the confidentiality of the PHI. This advisor will make the final decision on all claims appeals.

HR department employees may receive documents relating to an appeal electronically from a third-party administrator. These will be transmitted to the HR department via secure e-mail following the third-party administrator's security protocol.

## Section 1.04 Permitted Use and Disclosures Procedure

Consistent with guidelines set forth in the Privacy Rules, the county will respond to such a request only if the use or disclosure meets the following conditions:

- The disclosure falls within one of the following categories, and the specific requirements set forth in the Privacy Rules have been followed (45 CFR § 164.512):
  - in response to an order of a court or an administrative tribunal
  - in response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal, if there is an appropriate protective order in place and, where medical records are involved, the individual has waived their physician-patient privilege
  - pursuant to process (such as a court-ordered warrant or an administrative summons) and as otherwise required by law
  - to a law enforcement official (1) about an individual who has died; (2) for identification and location purposes; (3) about an individual who is, or is suspected of being, a victim of a crime; or (4) about an individual relating to a crime on the county premises
  - about an individual that the county reasonably believes is the victim of abuse, neglect, or domestic violence, to a government authority, including a social service or protective service agency, that is authorized by law to receive such information
  - to appropriate public health authorities for public health activities
  - to a health oversight agency for health oversight activities
  - to coroners, medical examiners, and funeral directors about a deceased individual
  - for organ, eye, or tissue donation purposes
  - for certain research purposes, when the need for an authorization has been waived or is otherwise not required
  - to avert a serious threat to health or safety
  - about armed forces personnel to appropriate military command authorities
  - for national security and intelligence activities
  - for protective services to the President of the United States and other designated persons
  - to correctional institutions and law enforcement custodians
  - relating to workers' compensation or other similar programs established by law that provide benefits for work-related injuries or illness without regard to fault
- The county's HIPAA Privacy Officer approves the use or disclosure after consultation with legal counsel
- the disclosure complies with the minimum necessary standard or is specifically exempted from the minimum necessary standard.
- If the disclosure is to a public official, the county will verify the identity and authority of the public official using the procedures set forth in "Verifying the Identity of Those Requesting PHI."
- The county will check state laws for any additional restrictions on the right to use or disclose PHI

- The county will document the disclosure according to the "Documentation and Record Retention Requirements," except that documentation is not required if the disclosure is for:
  - national security or intelligence purposes under 45 CFR 164.512(k)(2); or
  - to correctional institutions or law enforcement custodians under 45 CFR 164.512(k)(5).

## Section 1.05 Privacy Officer Procedure

The Privacy Rules also require the county to appoint a contact person or office which is responsible for receiving complaints of privacy violations and who can provide more information about the Notice of Privacy Practices that the county is required to send to all participants in the Health Plan and provide to its patients. The HIPAA Privacy Officer (HPO) has overall responsibility for the privacy and security of PHI. The HIPAA Privacy Officer may be reached:

Risk Management
2100 Pontiac Lake Road
Waterford, MI 48328
Phone: 248-858-1000

In addition to a countywide HIPAA Privacy Officer, each department shall select a privacy and security representative to be accountable to manage compliance with the HIPAA Countywide Privacy and Security Rule Procedures for their area. This individual(s) will represent their respective departments on the HIPAA Compliance Committee (HCC).

The HIPAA Privacy Officer, at their discretion, may delegate responsibilities to another individual with appropriate experience to carry out the delegated duties. The procedures within this document identify the HIPAA Privacy Officer as the person responsible for taking certain actions, the references include any individuals to whom the HIPAA Privacy Officer has delegated responsibility.

## Section 1.06 Disclosure Request Procedures

### (a) Disclosures Subject to Authorization Procedure

The county may provide individuals an authorization form that can be used to designate family members or others who are permitted to access the individual's Health Plan or medical record. The individual can, at any time, revoke their designation or authorize additional persons to whom the individual's PHI should be disclosed. These authorization forms and any subsequent revocations will be kept with the Health Plan records or medical records, as applicable.

### (b) Information About Deceased Individuals Procedure

If the county receives a request for information from a family member, other relative, or a close friend of the individual who were involved in the individual's care or payment for health care prior to the individual's death, the county, at its discretion, may disclose the information relevant to that person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the county.

### (c) Verification Procedure

If the county receives a request for a disclosure from a person claiming to have authorization to access an individual's Health Plan record or medical record, the county will check the applicable Health Plan or medical records to determine if the individual has signed an authorization giving this person access to the individual's PHI. If the person is not authorized to receive the PHI, the county may not make the disclosure, except that either parent of a minor child may access the minor child's records without an authorization unless the Health Plan has received a copy of a court

order prohibiting such access. The county employee receiving the request should verify the validity of the authorization using the procedures under "Uses and Disclosures of PHI with an Individual's Authorization."

### (d) Emergency Information Disclosure Procedure

If the county receives a request for information from a person who has not been identified in an authorization form to receive an individual's PHI (and is not otherwise authorized to receive the PHI for purposes of administering the Health Plan or providing health care), the county will normally deny the request. In an emergency, the Privacy Officer may permit disclosure to a family member or close friend who is involved in the individual's care or payment for the individual's care, if (1) the individual is aware that such disclosure may be made, has had an opportunity to object to the disclosure and does not object; or (2) the county is unable to notify the individual about the proposed disclosure and the Privacy Officer determines that the disclosure is in the individual's best interest.

## Section 1.07 Breach Procedures

### (a) HIPAA Incident Investigation Procedure

If a county workforce member detects or otherwise learns of an event involving PHI, they will notify their leader or HIPAA Working Group member. The HIPAA Privacy Officer will investigate the event consistent with this procedure. A HIPAA event becomes an incident upon investigation by the Privacy Officer and respective response team(s). If the incident involves Health Plan or medical records, the respective business unit will notify the Privacy Officer. Any county workforce member who learns of an incident involving unauthorized access to PHI (whether in electronic or paper form) will also notify the Privacy Officer of the event.

Upon notification of an event of unauthorized access to Health Plan or medical records, the Privacy Officer will determine whether the county has a duty to notify individuals of a breach. In determining whether notification is required, the Privacy Officer may consult with legal counsel, employees, agents, contractors, or consultants as reasonably necessary to determine the county's notification obligations, if any.

### (b) Breach Determination Procedure

The following are examples of the types of situations that may need evaluation. This evaluation includes scenarios in which a business associate notifies the county that an impermissible use or disclosure has or may have occurred:

- The county learns that an unauthorized individual has gained access to the county's electronic information system.
- The county learns that an authorized individual may have accessed protected health information for an improper purpose.
- The county learns that a portable device containing Health Plan or medical record information has been lost or stolen.
- The county learns that information intended for an authorized individual was misdirected (for example, by e-mail or fax transmission).
- The county learns that a business associate has suffered a potential data breach.
- The county hears from individuals who are the subject of protected health information that they have been the victims of identity theft or other identity fraud crime.

If a situation requires evaluation, the HIPAA Privacy Officer shall gather details about the incident, including the following:

- Specific data that is involved in the incident.

- Whether the access, use or disclosure is consistent with the county's HIPAA policies and procedures.
- Method the information was accessed, used, or disclosed, and the circumstances surrounding the incident.
- Date the incident was discovered.
- Date(s) the incident occurred.
- Number of individuals whose information was disclosed.
- Impacted individuals' state of residence.

When the HIPAA Privacy Officer learns of a possible breach of either its electronic files or physical files, they must first determine whether there has been an impermissible use or disclosure of unsecured protected health information under HIPAA's Privacy Rule.

If the facts indicate that the access, use, or disclosure was not permitted under HIPAA, the Privacy Officer will need to determine whether the incident falls into one of the exceptions to the HIPAA breach notification requirements. The county may not have a duty to notify if (1) the information is considered "secured"; (2) the incident is not considered a "breach"; or (3) the protected health information has not been compromised, as described below.

Note: While much of this policy addresses breach notification requirements under HIPAA, most states have security breach notification requirements that may also apply. Therefore, the Privacy Officer may need to consult with legal counsel to determine if the county has any obligations under state notification laws—whether notification is required under HIPAA.

Note: In the event of a breach, the county will also need to evaluate the effectiveness of its privacy and security practices and determine whether changes need to take place, consistent with the county's HIPAA evaluation procedures.

Determine whether information is deemed "secured" under HIPAA
The first step is to determine whether the information was properly secured under HIPAA. Whether the information is properly secured will depend on the nature of the information and how well it is protected.

If the information is electronic, the data is considered secured if both of the following are true:

- The data has been properly encrypted consistent with guidance issued by the Department of Health & Human Services.
- The individual/entity with improper access to the information does not have access to the confidential decryption process or key.

Data that has been destroyed may also be considered secured if one of the following is true:

- The information was stored on paper, film or other hard copy media, and the media has been shredded or destroyed in such a way that the protected health information cannot be reconstructed. (Note that redaction is **not** an effective form of destruction.)
- The information is in electronic form and has been cleared, purged, or destroyed consistent with National Institute of Standards and Technology (NIST) standards, so that the protected health information cannot be retrieved.

If the information meets one of the tests above for being secured, the incident will not be considered a breach and notification will not be necessary.

If the Privacy Officer concludes that the information is secured, they must document the facts leading to this conclusion and retain the documentation for a period of at least six years.

Determine whether incident falls within an inadvertent acquisition or disclosure exception

If the information is not considered secured, the incident may still not be considered a breach if the incident falls within one of the following exceptions:

Unintentional acquisition, access or use of protected health information

For this exception to apply, all the following must be true:

1. The unauthorized acquisition, access or use of protected health information must have been unintentional;

2. The individual who acquired, accessed, or used the protected health information must be one of the following:

   - a member of the county's workforce
   - A member of a business associate's workforce
   - A person acting under the authority of the county or the county's business associate

3. The individual who acquired, accessed, or used the protected health information did so in good faith.

4. The acquisition, access or use did not result in any further use or disclosure that is not permitted under the HIPAA privacy rules.

Inadvertent internal disclosure of protected health information
This exception applies if all the following are true:

1. Disclosure is made by an individual who is authorized to access protected health information.

2. Disclosure is made to an individual who is authorized to access protected health information.

3. Both individuals work for the same organization, which may be one of the following:

   - The county
   - The county's business associate
   - An organized health care arrangement in which the county participates

4. Disclosure did not result in any further use or disclosure that is not permitted under the HIPAA privacy rules.

Where the information would not be retained
This exception applies if all the following are true:

- Disclosure is made to an unauthorized individual.
- The county or its business associate has a good-faith belief that the unauthorized individual would not reasonably have been able to retain the information.

If the HIPAA Privacy Officer concludes that the incident meets one of the exception tests above, the incident will not be considered a breach and notification will not be necessary. The HIPAA Privacy Officer must document the analysis leading to this conclusion and retain the documents for a period of at least six years.

Determine the probability that the PHI has been compromised

If the HIPAA Privacy Officer determines that the information did not meet the requirements for being secured or fall within one of the exceptions noted above, the Privacy Officer must conduct a risk assessment. There is a presumption that an impermissible use or disclosure is a breach unless it can be determined through a risk assessment that there is a low probability that the PHI has been compromised.

Factors to consider include:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
    - Inclusion of Social Security numbers, driver's license numbers, bank account/credit card numbers, insurance numbers, or other PHI that could be used for identity theft or identity fraud crimes.
    - Inclusion of information about medical treatment, diagnoses, diseases, or similar details about an individual's health.
    - Likelihood that the PHI could be re-identified based on the context and the ability to link the information with other available information.
- The unauthorized person who used the PHI or to whom the disclosure was made
    - Whether the recipient was a HIPAA covered entity with a legal duty not to misuse the information.
    - Whether the recipient has a contractual relationship with the county that prohibits it from misusing the information.
    - Whether other facts and circumstances that would indicate that the recipient of the information is unlikely to misuse the information.
- Whether the PHI was acquired or viewed
    - Does a forensic analysis indicate that PHI on a lost computer was never accessed, viewed, acquired, transferred, or otherwise compromised?
- The extent to which the risk to the PHI has been mitigated
    - Whether there past dealings with the recipient or other factors that would indicate that the recipient can be trusted not to use or further disclose the information.

The HIPAA Privacy Officer should consider these and other pertinent facts to determine whether there is a low probability that the PHI has been compromised.

If the HIPAA Privacy Officer concludes that there is a low probability that the PHI has been compromised, then notification is not required. The HIPAA Privacy Officer must document the analysis leading to this conclusion and retain this documentation for at least six years.

## (c) Business Associate Breach Notification Procedure

Under HIPAA, a business associate who maintains protected health information on behalf of the county has a duty to notify the county of the breach within 60 days, but it is the county's duty to provide notification to the individuals

impacted by the breach. Moreover, in certain circumstances, the county may be charged with the business associate's knowledge of the breach, so that the deadline for providing notice will be based upon when the business associate knew or should have known about the breach.

To reduce the risk to the county of a HIPAA violation, the county will seek to include in its business associate agreements a provision that requires the business associate to notify the county of a potential breach within 5 business days of discovery and to provide information about the individuals involved in the potential breach within 30 days of discovery. Where appropriate, and after reaching consensus with the business associate, the county may also include a provision in the business associate agreement allocating responsibility for notification to individuals by the business associate. When a business associate reports a potential breach to the county, the HIPAA Privacy Officer will work with the business associate to determine whether the incident requires notification.
Notification

If the HIPAA Privacy Officer determines that the county must provide notification of the incident, the impacted department will prepare appropriate notification as required below.

## (d) Individual Notice Procedure

Under HIPAA, the county must provide notice to affected individuals without unreasonable delay, but no later than 60 days after the date the county discovers the breach or should have discovered the breach if it had exercised appropriate diligence. To reduce the risk of exceeding the deadline, the county will seek to provide notice as soon as reasonably possible once it has discovered the breach.

The HIPAA breach notification regulations require that the following information be included in the notification:

- Brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
- Description of the types of unsecured protected health information that were involved in the breach.
- Steps the individual should take to protect themselves from potential harm resulting from the breach.
- Brief description of what the county is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches.
- Contact procedures for individuals to ask questions or learn additional information including a toll-free telephone number, an e-mail address, Website, or postal address.

All notifications must be written in plain language.

Notice may be provided by e-mail to individuals who have agreed in advance to receive electronic notice. Otherwise, notice must be sent via first class mail. If the county knows that an individual is deceased and has the address of the deceased's next of kin or personal representative, the county may send the written notification to either next of kin or the personal representative.

Under HIPAA, the county has no more than 60 days after discovery of the disclosure to notify individuals. The date of discovery is measured as follows:

- First day the breach is known to a member of county's workforce or agents;
    - workforce member includes any employee, volunteer, trainee, agent, etc.
- First day a member of the county workforce or its agents **would have known** of the breach by exercising reasonable diligence; or

- First day that the county is notified of a breach by any of its independent contractors (unless the independent contractor is deemed to be an agent, in which case the county is deemed to have notice on the date the breach is first known to the independent contractor).

**Note:** State security breach notification laws may also apply and may mandate a shorter time frame for notification.

If the county does not have sufficient contact information for some or all the affected individuals (or if the contact information is outdated) then the county must provide substitute notice for such individuals in the following manner:

- If fewer than 10 individuals are affected, substitute notice can be provided to these individuals via telephone or other written notice that is reasonably calculated to reach the individuals.
- If more than 10 individuals are affected, HIPAA requires the following:
    - a conspicuous posting for a period of 90 days on the county's home page **or** a conspicuous notice in a major print or broadcast media in the geographic areas where the individuals affected by the breach likely reside; and
    - a toll-free phone number active for 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.
- The content of the substitute notice must include all the elements required for the standard notice described above.
- Substitute notice is not required in situations where an individual is deceased, and the county does not have sufficient contact information for the deceased individual's next of kin or personal representative.

If the county believes that there is the possibility of imminent misuse of unsecured protected health information the county may also provide expedited notice by telephone or other means. This notice is in addition to, and not in lieu of, direct written notice.

The county must retain copies of all notifications for at least six years from the date the notifications were provided. For substitute notifications, the county will retain copies for at least six years from the date the notification was last posted on the website or the date the notification last ran in print or broadcast media.

## (e) External Notification Procedures

### (i) Media Notification Procedure

If the HIPAA Privacy Officer determines that notification is required to more than 500 residents of a state, the county must provide notice in the form of a press release to prominent media outlets serving the state. The press release must include the same information required in the written notice provided to individuals. The Privacy Officer may coordinate such notice with the county's public relations department or other public relations consultants, as appropriate.

**Note:** State security breach notification laws should also be consulted to determine whether there are additional notification obligations to the media, state agencies, or national credit bureaus.

The county must retain copies of all press releases provided to prominent media outlets for at least six years from the date the notifications were provided.

### (ii) Department of Health & Human Services Notification Procedure

If the HIPAA Privacy Officer determines that the county or its business associate must provide notification to individuals under HIPAA, then the county will also have to provide notification to the Department of Health & Human Services. The timing of the notification will depend on the number of individuals affected by the incident:

- If the breach involves more than 500 individuals (regardless of whether they reside in the same state or in multiple states), the county will notify the Department of Health & Human Services without unreasonable delay, but no later than 60 days after discovery. This notification is to be submitted to the Department of Health & Human Services contemporaneously with the written notifications sent to individuals and in the manner specified on the department's website.
- If the breach involves fewer than 500 individuals:
    - The Privacy Officer must maintain a log of notifications involving fewer than 500 individuals. The information to be recorded in the log will be set forth on the Department of Health & Human Services' website.
    - The Privacy Officer will submit information from the log to the Department of Health & Human Services for each calendar year by February 28 of the following year, in the manner specified on the Department's website.

Notifications to the Department of Health & Human Services, including the annual log of notifications, must be maintained for at least six years from the date submitted to the Department.

# Section 1.08 Business Associate Procedures

Uses and Disclosures of PHI by Business Associates

The county may provide PHI to a business associate under the following conditions:

- the county has verified that a valid business associate contract is in place
- the disclosure is consistent with the terms of the business associate agreement (BAA)
- the disclosure complies with the minimum necessary standard (see Minimum Necessary Standard Addendum)

## (a) Business Associate Compliance Review Procedure

Prior to granting initial access to PHI and on a periodic basis, the county will ensure business associates have administrative, physical, and technical safeguards in place consistent with the terms of the (BAA) and Security Management Process/Evaluation standards in §164.308(a)(1), §164.308(a)(8), respectively. This includes but is not limited to:

- Verification of secure configuration of systems and physical locations
- Verification of documented policies and procedures to protect PHI
- Validation of HIPAA compliance training for employees

If a business associate is not able to submit documentation or if security controls does not meet requirements remediation will be documented in a corrective action plan.

## (b) Documenting Uses and Disclosures of PHI to Business Associates Procedure

Disclosures to business associates normally do not need to be documented, as such disclosures are typically made for payment, treatment, or health care operations purposes and thus exempt from the disclosure accounting requirements. If the county receives a request from a third party to use or disclose PHI for a purpose other than treatment, payment of claims or administration of the plan, the HIPAA Privacy Officer must approve such request before the use and disclosure is permitted and the county will document the use and disclosure in accordance with the "Documentation and Record Retention Requirements Procedure."

## (c) Unauthorized Uses and Disclosures of PHI by Business Associates Procedure

If the county learns that a business associate has used or disclosed PHI in an unauthorized manner, the county will take the following steps:

- the HIPAA Privacy Officer will immediately contact the business associate to discuss the alleged unauthorized use or disclosure and to determine whether the unauthorized use or disclosure will cease.
- if the business associate does not agree to stop the unauthorized use or disclosure, if the county learns that the use or disclosure has not stopped, or if the unauthorized use or disclosure is part of a pattern of conduct in violation of the business associate's agreement with the county, then the county will:
  - terminates its relationship with the business associate; or
  - if termination is not possible (for example, because there is no other service provider that can immediately provide the service), then the county may report the business associate to HHS.
- the HIPAA Privacy Officer will document the known details of the unauthorized use or disclosure for purposes of responding to requests for an accounting of disclosures
- if appropriate, the Privacy Officer will follow the procedures set forth in "Mitigation of Inadvertent Disclosures of PHI"
- the HIPAA Privacy Officer will follow the Breach Notification Policy contained in the county's Security Policies and Procedures, as needed

# Section 1.09 Complaints Procedure

The HIPAA Privacy Officer will investigate all situations involving a suspected breach or other impropriety. Upon receiving a complaint, the Privacy Officer will do the following:

- review the Policies and Procedures or Privacy Rules at issue
- obtain any additional information from the individual necessary to understand the nature and basis of the complaint
- investigate the conduct that is the subject of the complaint, which may include interviewing members of the workforce and business associates, and reviewing records in the individual's record
- if appropriate, consult with legal counsel or other appropriate resources for evaluating the complaint
- decide how the complaint will be handled and then take appropriate action within thirty days of receiving the complaint, which may include:
    - actions necessary to minimize any harmful effects from the unauthorized use or disclosure, including taking any actions required by the Breach Notification Policy contained in the county's Security Policies and Procedures
    - disciplinary action against employees in accordance with the county's disciplinary practices
    - appropriate actions with respect to business associates in accordance with the relevant business associate agreement
    - modification of the Policies and Procedures, if necessary
    - no action, if it is determined that there has been no violation of the Policies and Procedures or the Privacy Rules
- communicate to the individual, in writing and on a timely basis, the outcome of the complaint investigation
- retain documentation of the complaint and its disposition as required by documentation and record retention requirements

If the HIPAA Privacy Officer was involved in the activity that is the subject of the complaint, the HIPAA Privacy Officer will appoint a person not involved in the activity and who does not work directly for this role to handle the complaint.

## Section 1.10 Documentation and Record Retention Requirements Procedure

### (a) HIPAA Documentation Procedure

The county will maintain a copy of HIPAA policies and procedures for six years beyond the date the documents cease to be effective.

### (b) Notice of Privacy Practices Documentation Procedure

The county will maintain a copy of Notice of Privacy Practices for six years beyond the date the documents cease to be effective.

### (c) PHI Disclosure Documentation Procedure

The Privacy Rules require that certain uses and disclosures be documented so that the county can respond to an individual's request for an accounting of disclosures. To comply with this requirement, the county will keep records of the following information for certain types of disclosures:

- the individual whose PHI was disclosed
- the date of the disclosure
- to the extent known, the name and address of the entity or person who received the PHI
- a brief description of the PHI disclosed
- a brief statement of the purpose of the disclosure

To properly account for uses and disclosures, the information identified above must be kept for a period of six years for the following types of disclosures:

- all unauthorized disclosures known to the county
- disclosures to law enforcement
- disclosures to HHS
- any disclosures required by law, including those made:
    - in response to the order of a court or an administration tribunal
    - in response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal, if there is an appropriate protective order in place and, where medical records are involved, the individual has waived their physician-patient privilege
    - pursuant to process (such as a court-ordered warrant or an administrative summons), and as otherwise required by law
- any of the following permitted disclosures:
    - to a law enforcement official (1) about an individual who has died; (2) for identification and location purposes; (3) about an individual who is, or is suspected of being, a victim of a crime; or (4) about an individual relating to a crime on the county premises
    - about an individual that the county reasonably believes is the victim of abuse, neglect, or domestic violence, to a government authority, including a social service or protective service agency, that is authorized by law to receive such information
    - to appropriate public health authorities for public health activities
    - to a health oversight agency for health oversight activities
    - to coroners, medical examiners, and funeral directors about a deceased individual
    - for organ, eye, or tissue donation purposes
    - for certain research purposes, when the need for an authorization has been waived or is otherwise not required
    - to avert serious threat to health or safety
    - about armed forces personnel to appropriate military command authorities
    - for protective services to the President of the United States and other designated persons

- to correctional institutions and law enforcement custodians
- relating to workers' compensation or other similar programs established by law that provide benefits for work-related injuries or illness without regard to fault

The following uses and disclosures do not need to be documented for purposes of an accounting:

- to carry out treatment, payment, and health care operations
- to the individual that is the subject of the PHI (except formal requests to inspect and/or copy – see "Documenting Authorizations and Individual Rights" below)
- uses and disclosures incidental to permitted uses and disclosures
- pursuant to a valid authorization signed by the individual who is the subject of the use or disclosure
- for national security or intelligence purposes
- to correctional institutions or law enforcement custodians when the disclosure was permitted without an authorization

## (d) PHI Authorization Documentation Procedure

The county will maintain for a period of six years from the date the document was last effective, the following documents:

- Individual authorizations for use or disclosure of PHI
- Revocation of authorizations for use or disclosure of PHI
- With respect to an individual's request for an accounting:
  - temporary suspensions of an individual's right to an accounting requested by:
    - a health oversight agency conducting health oversight activities authorized by law, pursuant to 45 CFR § 164.512(d)
    - a law enforcement official, conducting an activity described in 45 CFR § 164.512(f)
  - communications extending the deadline to respond to the request
  - the written accounting provided in response to the request.
- With respect to an individual's request to inspect and copy PHI:
  - communications extending the deadline to respond to the request
  - communications denying in whole or in part a request to inspect and copy PHI
  - communications explaining the outcome of an appeal to review a decision denying a request to inspect and copy PHI.
- With respect to requests to amend PHI:
  - communications extending the deadline to respond to the request
  - communications denying in whole or in part a request to amend PHI
  - any statement of disagreement that an individual submits to the county in response to a decision denying a request to amend PHI.
  - any rebuttal statements that the county prepared in response to a statement of disagreement.
  - requests for amendment that are denied, if the individual who submitted the request asks the county to provide the request and denial with any future disclosures of the PHI.
  - Note: if the county elects to amend PHI, the amendment must be maintained if the record is maintained; if the county elects not to grant the amendment and the individual files a disagreement, the disagreement and any rebuttal statement must be maintained if the record is maintained, plus an additional six years.
- Additional restrictions requested by an individual to which the county agrees, and any terminations of such restrictions.
- individual complaints, and all documents relating to their disposition

The obligation to retain documents relating to individual rights is limited to requests made to the county for documents maintained by the county. When PHI is held by a county business associate, the individual will be referred to the business associate and the business associate is responsible for maintaining required documentation relating to individual rights.

In addition to the documents listed above, the county may at its discretion maintain any additional documents it believes are appropriate relating to requests by individuals to exercise their individual rights under HIPAA.

## (e) HIPAA Training Documentation Procedure

The county will maintain documentation demonstrating dates of training records for employees with access to PHI. Training will include applicable policies and procedures relating to the Privacy Rules, for a period of six years from the date each training session was concluded.

## (f) Complaints Documentation Procedure

The county will maintain documentation of all complaints that the county receives of violations of these policies and procedures related to the Privacy Rules, and all documentation relating to disposition of the complaints. The county will maintain these documents for six years from the date of a complaint's final disposition.

## (g) Disciplinary Action Documentation Procedure

The county will maintain documentation of all disciplinary action that the county has taken against its workforce members for violations of these policies and procedures related to the Privacy Rules, for a period of six years from the date of the disciplinary action.

## (h) BAA Documentation Procedure

The county will maintain copies of all business associate agreements for a period of six years from the date the contract was last in effect.

## Section 1.11 Individual Rights Procedures

### (a) Individual's Request to Inspect and Copy Procedure

The Privacy Rules give individuals the right to inspect and copy the records that the county maintains about them (see 45 CFR § 164.524). If an individual seeks information held by an insurer or third-party administrator, the county will instruct the individual to make the request directly to the insurer or third-party administrator. If the county maintains the requested information, it will respond to the request using the following procedures.

The county generally maintains limited information about individuals covered under the Health Plan and this information may generally be accessed without restrictions. If the county maintains records for which the Privacy Rules do not allow a right to access (see 45 CFR § 164.524(a)(1)), the county will not provide access to the records. When denying a request for access, the county will follow all procedures outlined in the Privacy Rules including providing timely written notice to the individual and permitting a review of the determination where appropriate.

If the county maintains the PHI in an electronic form, the county must be able to provide the PHI in an electronic form to an individual. The county must provide the individual with access to the PHI in the electronic format requested by the individual if it is readily producible in that format. If the county cannot provide the information in the requested format, it will offer to produce the information in the formats that are available. If the county and the individual cannot agree on an electronic format, the county may produce the records in paper form.

If an individual's request for access directs the county to transmit a copy of the PHI to another person designated by the individual, the county must provide a copy to the person designated by the individual. The individual's request must: (1) be in writing; (2) signed by the individual; (3) clearly identify the designated person; and (4) clearly identify where to send the copy of PHI. The request does not need to comply with the Authorization requirements.

For approved requests, the county will provide access in a timely manner in accordance with the Privacy Rules. The county may impose a reasonable fee for providing copies or summaries of PHI. If imposed, the fee will only include: (1) the cost of copying, including the cost of supplies for and labor of copying (including cost of portable media, if the individual requests an electronic copy); (2) postage, when the individual has requested that the copy, or the summary or explanation, be mailed; and (3) expenses incurred in preparing an explanation or summary of the PHI, if the individual agrees. The county will maintain required documentation in accordance with the Documentation and Record Retention Requirements Addendum.

The Privacy Rules give individuals the right to request an amendment of their records that the county maintains (see 45 CFR § 164.526). If the individual seeks information held by an insurer or third-party administrator, the county will instruct the individual to make the request directly to the insurer or third-party administrator. If the county maintains the requested information, it will respond to the request using the following procedures.

Individuals seeking to amend Health Plan or medical records maintained by the county must provide a reason to support the requested amendment. The county must either comply with or deny the individual's request for an amendment no later than 60 days after receipt of the request. If the county is unable to act on the amendment request within 60 days after the receipt of the request, it may seek to extend the time for its decision no more than 30 days if, within the original 60-day time limit, it provides the individual with a written statement of the reasons for the delay and the date by which the county will make its decision. The county may have only one extension of time.

The county is not obligated to grant the individual's request. The county may deny an individual's request to amend the Health Plan or medical record in the following circumstances:

- The protected health information or record was not created by the county (for example, it came from another health care provider, an insurer or third-party administrator)—unless the originator of the information is no longer available to act on the request;
- The record is not part of the designated record set;
- The information would not be available for inspection under the right of access (for example, because it was compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding);
- Or because the information is accurate and complete.

If the request for amendment is denied, in whole or in part, the county will provide a timely, written denial that explains in plain language the basis for the denial and explains the individual's right to submit a statement of disagreement. If the individual submits a statement of disagreement, the county may prepare a written rebuttal and send a copy to the individual who submitted the statement of disagreement. If the county makes any subsequent disclosure of the protected health information at issue, the county must include the individual's request for amendment, the denial, and any statements of disagreement and rebuttal (or an accurate summary of such information).

If the request for an amendment is accepted, in whole or in part, the county will identify the records affected by the amendment and append or otherwise provide a link to the location of the amendment. The county will also inform the individual who requested the amendment that the amendment is accepted, determine from the individual whether others need to be informed of the amendment, and then make reasonable efforts to inform the necessary individuals that the amendment has been made. In the event the county is informed of an amendment made by a health care provider, another health plan, or a Business Associate, the county will determine whether it must amend the PHI in its own Health Plan or medical record accordingly.

The county will maintain required documentation in accordance with the Documentation and Record Retention Requirements Addendum.

## (b) Individual PHI Request Disclosure Procedure

The Privacy Rules give individuals the right to request an accounting of disclosures of their PHI. If the individual seeks an accounting of disclosures made by an insurer or third-party administrator, the county will instruct the individual to make the request directly to the insurer or third-party administrator. If the individual seeks an accounting of disclosures made by the county, the county will respond to the request using the following procedures.

An individual may request an accounting of disclosures for a period of up to six years from the date of the request. The county must provide a written accounting or a written notification of an extension of time no later than 60 days after receipt of such a request (see 45 CFR § 164.528). Any fees for providing the accounting will be in accordance with the Privacy Rules.

The county will suspend an individual's right to receive an accounting of disclosures, in accordance with the Privacy Rules, upon receiving an appropriate request from a health oversight agency or law enforcement official for the time specified by such agency or official (see 45 CFR § 164.528(a)(2)).

The county will maintain required documentation in accordance with the Documentation and Record Retention Requirements Addendum.

## (c) Individual Confidential Communications Request Procedure

Individuals may request that the county communicate with them through alternative means or at alternative locations (see 45 CFR § 164.522(b)). All requests must be made in writing. The county may condition the provision

of a reasonable accommodation on how payment, if any, will be handled and the specification of an alternative address or other method of contact.

For Records Related to the Health Plan
The county's policy is to accommodate all reasonable requests for confidential communications as required by the Privacy Rules if the individual clearly states that the disclosure of all or part of that information could endanger the individual. The county may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

For Records Related to the Provision of Health Care
The county's policy is to accommodate all reasonable requests for confidential communications as required by the Privacy Rules. The patient will be notified of the right to request communication by alternative means or an alternative location in the county's Notice of Privacy Practices. The county will not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

## (d) Individual Restrictions on PHI Uses and Disclosures Request Procedure

The Privacy Rules give individuals the right to request that the county restrict its uses or disclosures of their PHI beyond the restrictions imposed by the Privacy Rules. If an individual seeks to restrict an insurer's or third-party administrator's use of PHI, the county will instruct the individual to make the request directly to the insurer or third-party administrator. If an individual seeks to restrict the county use of PHI, the county will respond using the following procedures.

The Privacy Rules do not require the county to agree to any requested restrictions except as described below. Moreover, the county will not agree to a request to restrict a use or disclosure that the county is required to make under the Privacy Rules or that it is otherwise required by law to make.

If the county agrees to a restriction, it may not use or disclose PHI contrary to such restriction. The county, at its discretion, will only agree to a requested restriction if it and its insurers or third-party administrators can comply with the restriction without additional cost or administrative burden. The county may terminate an agreed-upon restriction only in a documented agreement with the individual or with notice that applies only to PHI created or received after the individual receives the notice.

## (e) Mandatory Restrictions Procedure

The county must agree to an individual's request to restrict disclosure of their PHI if (1) the disclosure is for carrying out payment or health care operations and is not otherwise required by law; and (2) the PHI pertains solely to a health care item or service for which the individual or person other than the health plan, on behalf of the individual, has paid the county in full.

If the county has agreed to a restriction, it may use the restricted PHI or may disclose the restricted PHI to a health care provider to provide emergency treatment to the individual if the individual who requested the restriction needs emergency treatment and the restricted PHI is needed to provide the emergency treatment. The county must request that such health care provider not further use or disclose the information.

The county will maintain required documentation in accordance with the Documentation and Record Retention Requirements Procedure.

# Article I. HIPAA Security Rule Procedures

## Section 2.01 Information Access Management Procedures

### (a) Health Care Clearinghouse Functions Procedures

The county does not perform any healthcare clearinghouse functions and accordingly is not subject to the Isolating Healthcare Clearinghouse Functions standard in 45 CFR § 164.308(a)(4)(ii)(A).

### (b) Workforce Clearance Procedure

Reasonable clearance processes will be used to determine that a workforce member's access to information systems is appropriate. The following clearance processes will take place:

- Before an individual is hired, that person's job references will be checked.
- Before any employee/contractor is given access to the county information systems, the employee will sign a non-disclosure agreement acknowledging they will be given access to restricted information during their employment/engagement with the county and acknowledging their obligation to maintain the confidentiality of such information.
- Before an employee/contractor is given access to ePHI, a criminal background check will be conducted and other validation methods to ensure access is appropriate

## Section 2.02 Information Authorization and Authentication Procedure

Access to PHI is guided by:

- determining that authorization is valid (as described below);
- verifying the identity of the individual who signed the authorization; and
- ensuring the use or disclosure is consistent with the terms of the authorization.

An authorization is valid only if it is written in plain language and contains the following required core elements and statements:

Core Elements

Authorization must contain all the following core elements:

- a specific and meaningful description of the PHI to be used or disclosed
- the name or other specific identification of the person or class of persons authorized to use or disclose the PHI
- the name or a description of the person or class of persons to whom the county may make the requested use or disclosure
- the purpose(s) of the requested use or disclosure. (If the individual initiates the authorization and does not provide a statement of purpose, the statement "at the request of the individual" is sufficient)
- a valid expiration date (e.g., December 31, 2014) or expiration event (e.g., termination from the Health Plan, rejection of an insurance application, etc.)
- the signature of the individual and the date the authorization was signed. (If signed by the individual's personal representative, a description of the representative's authority to act for the individual must also be provided)

Required Statements

Authorization must contain all the following statements:

- a statement of the individual's right to revoke the authorization in writing, and either (1) a list of the exceptions to the right to revoke and a description of how the individual may revoke the authorization; or

(2) a reference to the Notice of Privacy Practices, if the Notice lists the exceptions to the right to revoke and provides a description of how the individual may revoke the authorization

- a statement (as applicable) informing the individual that:
    - the county may not condition treatment, payment, enrollment, or eligibility for benefits on whether the individual signs the authorization; or the consequences to the individual if he or she refuses to sign the authorization when:
    - the authorization is to be used for the Health Plan's eligibility or enrollment determinations or for its underwriting or risk rating determinations, and the authorization is not for the use or disclosure of psychotherapy notes; or
    - a covered entity will be providing health care solely for creating PHI for disclosure to a third party and the authorization is to allow the disclosure to the third party (e.g., a physician releasing the results of pre-employment drug testing to the county)

**Note:** The individual authorization form, when correctly filled out, signed, and dated, should satisfy all the above requirements, and constitute a valid authorization under the Privacy Rules.

Providing a Copy of the Authorization to the Individual

If the county is seeking the authorization from the individual, the county must provide the individual with a copy of the signed authorization.

## Section 2.03 Limitations on Access Procedure

Authorized Employees are either involved in administering the Health Plan or in providing health care. Authorized Employees include:

- Privacy Officer/Security Officer
- HR department personnel involved in the administration of Health Plan benefits
- County attorneys, paralegals, and related support staff providing legal services to the Health Plan
- Information technology personnel providing support for Health Plan operations
- Nurses
- Physicians
- Case Managers
- Billing staff

These authorized employees may use and disclose PHI to perform or support treatment, payment and healthcare operations functions, Health Plan administration functions, and they may disclose PHI to other Authorized Employees who perform or support such functions and to third party administrators or other service providers who have a HIPAA business associate agreement (BAA) with the county. Such uses and disclosures, however, must be limited to the minimum necessary to perform or support such functions. Routine uses, and disclosures must be made in accordance with these Policies and Procedures. Non-routine uses, and disclosures must be approved by the Privacy Officer. Authorized employees must not disclose PHI to employees not identified in this section, except in accordance with these Policies and Procedures.

## Section 2.04 Access Authorization and Management Procedures

Where appropriate, county workforce members may be granted the following access rights to the county Information System:

- Delegated Department/IT System Administrator rights. In addition to general access rights, respective business unit staff (including IT) may be granted administrator rights to systems and applications, to create user IDs, and to delete users and mailboxes.

## (a) Access Authorization Revocation Procedure

An individual may revoke an authorization at any time, although the revocation will not be effective to the extent that the county has already used or disclosed information in reliance on the authorization.

## (b) Access Authorization and Supervision Procedure

Access to computer systems containing ePHI will be granted as follows:

When an employee begins work or changes roles at the county, the Human Resources department or respective business unit management will provide information to the IT department/business unit delegated department system administrator about the individual and their job responsibilities. The new employee's department will determine system access rights based on the job function. IT department/business unit delegated department system administrator will grant access rights for the newly-hired employee based on management's authorization.

When contractors begin work at the county, the contractor's department leadership will provide the IT department/business unit delegated department admin with the contractor's job role and responsibilities, along with system access rights. The IT department and/or business unit delegated department system administrator will grant access rights based on management's authorization.

The following procedures apply to access authorization:

- User accounts can only be assigned with respective department management or delegate approval
- Business unit management is responsible for requesting and maintaining an account of access for their staff whether employee or contractor
- All requests regarding user accounts or information system access will be communicated through the county's IT ticketing system for audit and accountability
- System administrators will only process requests authorized in writing by management or their delegates
- Records of access requests will be maintained per relevant state/federal and business requirements

When an existing employee changes job functions to a position that requires a different level of access to PHI stored in Oakland County Systems, the respective business unit manager will work with the IT department/delegated department system administrator to establish the appropriate level of access.

When an existing employee changes job functions to a position that requires changing or removing access to county information systems, the employee/contractor's respective business unit management will provide information to the IT department/business unit delegated department system administrator about the change in job function, the effective date of the change, the required change in access rights associated with the change in job function, and the date on which changes in access rights should go into effect.

When an existing employee changes job functions to a position that no longer requires access to county information systems, Respective business unit management will provide that same information to the IT department/business unit delegated department system administrator. IT department/business unit delegated department system administrator will change access rights to conform with the manager's written instructions.

## (c) Tracking and Logging Authorization for Access Procedure

The county will capture and monitor a log of unsuccessful log-in attempts as appropriate to its information systems.

The county does not grant third parties access to system resources without defined and documented business justification. Visitors are granted guest access to the Internet through a separate security system from other system resources with no access to the county's system resources. Any exception for access rights to system resources must be cleared by the HIPAA Privacy and Security Officers and respective business unit data owners. If

the third party will have access to PHI, the third party will first have to sign a HIPAA Business Associate and Non-Disclosure Agreements.

## (d) Workforce Termination Procedure

When a workforce member's employment/contract ends, that individual's privileges to access the information system will be disabled on a timely basis.
In the case of voluntary terminations:

- The employee's supervisor will ask the employee to provide written notice of the employee or contractor's last day of employment.
- Prior to the employee's last day of employment (when possible), the HR Employee Records Unit/contractor's business unit management will notify the IT Department and the IT Department will remove the individual's access rights to the information system (including the e-mail system).

In the case of an involuntary termination:

- Before the termination, the HR Employee Records Unit/ contractor's business unit management will coordinate with the IT Department on terminating the employee's access to the information system.
- Following the employee's departure, the workforce member's business unit management will check the employee's office/work area on a timely basis.

## (e) Access Termination/Suspension Procedure

Respective business unit management or their delegates are responsible for ensuring timely termination of a workforce member's access to PHI under the following circumstances outside of job change or termination:

- If management has evidence or reason to believe the individual is using information system resources inconsistent with terms of use under this policy
- If the workforce member's password has been compromised
- If the workforce member's workstation has been compromised

## (f) Emergency Access Procedure

Respective department-level privacy/security representatives are authorized to approve access to ePHI for appropriate individuals in emergency situations. Alternatively, the HIPAA Privacy and Security Officers can approve emergency access. IT department staff and respective delegated department system administrators will grant access and remove when no longer needed.

## (g) Periodic Access Review Procedure

The county will perform periodic access review to systems to ensure there is valid need to know. The process will involve respective business unit management and data owners.

## (h) User Identity and Authentication Procedure

The county uses reasonable processes to confirm that a user seeking access to the county's ePHI is who it claims to be. For internal or external access by workforce members, the user's unique user identification name and password will authenticate the individual's identity. The identity of any nonuser entity (e.g., another computer system) seeking access to the county's ePHI will be authenticated by a unique user identification name and password.

Users are given unique user identifications and passwords.

Users can change their password at a minimum after 24 hours. They are required to change system passwords every 90 days. The IT department will not change user passwords but will give users guidance on how to change their password.
When a user forgets their password, they shall contact the IT Department. The IT department will reset the password and allow the user to establish a new password.

## Section 2.05 Continuity Procedures

The following procedures outline mechanisms the county employs to address business continuity and system recovery.

### (a) Business Continuity Procedures

Respective business unit and IT management will maintain continuity plans for their area of responsibility to address resiliency in emergency conditions.

#### (i) Plan Testing and Revision Procedure

Plans will be tested periodically; and, revised when there is a significant change in regulatory/legal environment, operations, or technology.

#### (ii) Data Backup Plan Procedure

IT and respective business unit system and data owners will maintain a data backup plan.

The county will make reasonable measures to protect backup media and underlying data in various forms, as identified in the System Integrity Procedure.

## Section 2.06 Information Protection Procedures

### (a) Malicious Software Protection Procedure

Malicious software includes viruses, worms, adware/spyware, Trojan Horses, and other similar software designed to disrupt, deny, or modify information systems in an unauthorized manner.

The IT Department employs multiple technical, administrative, and physical controls to secure endpoints from malicious software. This includes antivirus software, security awareness training and periodic reminders, and other safeguards.

Workforce members granted access to Oakland county systems are prohibited from circumventing or modifying security settings. If a user identifies possible malicious software on their computer, the user should immediately notify the IT Department, which will then take appropriate steps to remediate.

### (b) Workstation Security Procedure

The county Information System utilizes a screen saver that has an automatic locking function after 15 minutes of inactivity. The screen saver is enabled as a default feature of the workstation. Users must re-login to their workstations upon engaging their system. Users are prohibited from circumventing or modifying security settings on their assigned workstations.

### (c) System Integrity Procedure

The IT Department uses secure measures where appropriate and feasible to protect ePHI from unauthorized disclosure or modification. Measures include encryption, password protection, event logging, and access controls. Authorized access to systems that store, or process PHI is provided in accordance with the Information Access Management section of this manual.

## Section 2.07 IT Security Management Procedures

County information is maintained through application of security controls, data management, and maintenance of the security infrastructure. This policy establishes requirements that assist management in defining a framework

to ensure a secure environment. This framework provides the overarching structure for safeguarding county information resources.

This policy applies to the county, its employees, contractors, vendors, other users, and information assets.

The county shall develop, implement, and manage a HIPAA Compliance program. To perform its execution, the county shall designate HIPAA Security and Privacy Officers. Related Procedures to address the HIPAA Security Management standard include:

- IT Documentation Management
- Assigned Information Security Responsibility
- Security Process Audit
- Risk Management

## (a) IT Documentation Management Procedure

The county shall establish a process by which HIPAA Security Rule Policies and Procedures are created and maintained per federal regulations.

The county is required to have policies and procedures to comply with HIPAA Security Rule requirements.

Policies and procedures shall be reviewed periodically, and revised upon:

- Changes in the operational or technology environment
- Federal regulation mandates
- Risk analysis

The county HIPAA Privacy and Security Officers shall direct the review and revision process. Corporation Counsel shall provide legal review of policies and procedures. Approval of the HIPAA IT department Security Rule Policies and Procedures will be made by the HIPAA Compliance Working Group in consultation with IT Steering.

All assessments, operational control execution, risk mitigation decisions shall be documented and maintained per HIPAA and relevant business retention requirements.

## (b) Assigned Security Responsibility Procedure

The county shall appoint a HIPAA Security Officer (HSO) who shall be responsible for developing and monitoring policies and procedures to address confidentiality, integrity, and availability of EPHI per HIPAA Security Rules. This function addresses regulatory compliance under this procedure adopted by the county. The HIPAA Privacy and Security Officers will co-chair the HIPAA Compliance Committee (HCC) and HIPAA Compliance Working Group (HCWG).

## (c) Security Process Audit Procedure

The HIPAA Security Officer and Privacy Officers will monitor the PHI security management process, status of compliance initiatives, and the county's adherence to related policies and procedures. The HIPAA Privacy Officer will report regularly on the status of the county's regulatory compliance to appropriate leadership.

The HIPAA Security Officer and other respective business unit staff will conduct a technical and nontechnical evaluation of IT processes in line with security policies and procedures on a periodic basis; or, whenever there is a significant change in the county's information systems that affect the security of ePHI. The HIPAA Security Officer, in consultation with respective business unit leadership, will determine the definition of a significant change to the county's information system. The evaluation will consider changes in the county's business, information systems environment, management, and operations. These policies and procedures may be revised as appropriate based on evaluation.

## (d) Risk Management Procedure

The county follows a risk management program intended to reduce the risks to the ePHI stored on its information systems to reasonable and appropriate levels. Risk management is an ongoing process. Strategies for managing risk should be commensurate with the risks to such systems, and may include the following methods: (a) system identification and characterization, (b) assessment of current and compensating administrative/physical/technical controls, (c) risk rating, and (d) risk prioritization and mitigation.

On a periodic basis (or upon changes occur in the county's environment), the county shall conduct an organizational risk assessment per industry best practice guidelines. Assessments include but are not limited to:

- Administrative (policies and procedures) safeguards
- Technical process and safeguards
- Physical security assessments
- Business associate compliance review

Under direction from the HIPAA Privacy and Security Officers, appropriate staff will regularly review records of activity on information systems containing ePHI. The county will implement and maintain appropriate hardware, software, or procedural auditing mechanisms on information systems that store or transmit ePHI. The HIPAA Security Officer in conjunction with respective business unit management will determine the appropriate level and type of auditing mechanism based on the risk analysis process, and will assign responsibility to an appropriate staff member to regularly review system activity records.

## (e) Sanction Procedure

Workforce members who violate policies and procedures governing the security of the county's computer systems are subject to discipline pursuant to the Oakland county Merit Rules. Contractors and vendors are subject to discipline pursuant to the contract, up to and including termination of their county contract.

## (f) Information Security Incident Handling Procedures

Information security incidents under HIPAA Security Rule involves any intentional or unintentional, suspected, or actual incident that affects the confidentiality, integrity, or availability of ePHI. Workforce members, vendors, or others are required to report incidents immediately to the HIPAA Privacy Officer and the IT Department as appropriate.

Examples of incidents include, but are not limited to:

- Misdirected fax, email, or print jobs
- Lost or stolen electronic mobile devices (smartphone, laptop, tablet) or removable media (CD, USB drives)
- Unauthorized modification of PHI
- Malware attacks
- Suspected or actual network intrusion attempt
- Unauthorized access to ePHI or system that stores ePHI
- Lost or stolen electronic ID badges, office/building keys
- Unauthorized persons in secure areas

### (i) Response and Resolution Procedure

The HIPAA Privacy Officer and Corporation Counsel shall evaluate reported incidents to determine if a breach of ePHI occurred. If a breach has occurred, the Privacy Officer shall engage the HIPAA Security Officer, Information Technology, Human Resources, county media contacts or law enforcement as deemed necessary.

The Privacy Officer shall coordinate appropriate notification under Breach Notification requirements with the HIPAA Security Officer, as applicable.

Whenever a significant security incident has been identified, the responsible IT staff member shall document additional details about the incident to include as much of the following information as is known:

- The date the security incident was discovered and the steps taken to research details of the incident
- The date and time of the incident
- The ePHI involved in the incident, including the specific names of individuals whose data was involved.
- The origin of the activity
- The user performing the activity
- Individuals who were contacted about the significant security incident
- Any steps taken to mitigate harmful effects of the incident

With documented approval from the Chief Information Security Officer (CISO) and HIPAA Privacy/Security Officers, copies of such reports will be given to management, and if the security incident results in a workforce member being sanctioned then the county will receive a copy of the report for the individual's personnel file. Any security incident report sent to the HR department will have any PHI appropriately redacted. Corporation Counsel and/or the HIPAA Privacy Officer will retain the security report of a significant security incident event for a minimum of seven years.

#### *(ii)* Risk Management Effectiveness Evaluation Procedure

Whenever a significant security incident has occurred, the HIPAA Security Officer will evaluate current risk management methods in use and determine whether an alternative method should be employed, and report their findings and recommendations to the CISO and IT Steering.

### (g) Security Training and Awareness Procedures

#### (i) County Employee Training Procedure

All county employees are required to take HIPAA compliance training, which includes privacy and security concepts. Targeted PHI handling training is required for staff that access or handle this restricted data classification prior to gaining access. Reminder training for existing employees will be done on an annual basis through a variety of methods. Documentation of HIPAA training will be kept in a central repository.

#### (ii) Non-employee Training Procedure

Contractor and vendor training will be in accordance with the 'Business Associate Compliance Procedure.' Training for unpaid interns, volunteers, and other non-employees will be handled through respective county department leadership.

#### (iii) Targeted Training for Data Custodians Procedure

The county will ensure targeted training for IT staff and delegated department system administrators in applying safeguards to systems that store, transmit, or process PHI.

#### (iv) Security Reminders Procedure

Periodically, the county will review privacy and security topics with employees to reinforce training. Online training and other content will be posted and available to workforce members on the county's intranet site.

## Section 2.08 Facility Access Procedures

#### (i) General Access Controls, Security, and Validation Procedure

The county shall employ the use of electronic access cards to secure areas. Outside of business hours, employees and authorized contractors/vendors will use their county ID to swipe their badges for entry into Oakland County

buildings. Individuals entering the building without an ID are required to sign in at the reception desk. An escort is required for individuals entering secure areas of county buildings.

### (ii) Additional Protection of Electronic Information Systems and Maintenance Logs Procedure

Other physical security controls include the following requirements:

- Secure area access authorization must follow a formal process which includes written permission from respective area management.
- Logs of visitor access to building and secure areas must be captured and maintained.
- All contracted hardware maintenance personnel entering secure areas must sign-in.
- All county Employees and Consultants must display their county issued ID badge on their person.
    - If lost or stolen, workforce members must report to respective area management immediately.
- Anyone without a county ID card MUST sign in at the reception desk, and obtain a temporary ID card.
- All visitors must be escorted from and to the lobby.

## Article II. References

Oakland County HIPAA Policy
Oakland County Health Division Privacy Practices
HIPAA Privacy Rule
HIPAA Security Rule
HIPAA Breach Notification Rule
HITECH
Security Rule Guidance Material
National Institute of Standards and Technology Special Publication (NIST) 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems

## Article III. Definitions

| Term/Acronym | Definition |
|---|---|
| Administrative Safeguards | Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information. |
| Authentication | The corroboration that a person is the one claimed. |
| Authorization | Function of specifying access rights to resources related to information |
| Availability | The property that data or information is accessible and useable upon demand by an authorized person/user entity. |
| BAA | Business Associate Agreement. |
| BA | Business Associate. |
| Breach | The acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. |
| Business Associate | A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. |
| CMS | Center for Medicaid and Medicare Services |
| Confidentiality | The property that data or information is not made available or disclosed to unauthorized persons or processes. |
| Contractor | An individual employed and managed by a third party, but uses Oakland County information resources to perform work on behalf of the County. They are subject to information protection rules and contractual obligations. |
| County-owned Asset | Information, data, hardware and software, facilities, and equipment owned, leased, purchased, or developed on behalf of the county. |
| Covered Entity | The entity under HIPAA that provides or manages health care services. A covered entity may be a hybrid, meaning they may have only a healthcare portion but other business. Under HIPAA, only the healthcare portion is subject to this regulation. |
| Covered Function | Functions of a covered/hybrid entity, the performance of which makes the entity a health plan, health care provider, or health care clearinghouse. |
| Disclosure | Release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information. |

| | |
|---|---|
| | (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission. |
| Electronic Media | Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card |
| Employee | An individual who is paid and managed by the County. The term employee when used in the Policies and Procedures will be included as part of the County's workforce. |
| Encryption | The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. |
| E-PHI | Electronic protected health information. See PHI definition. |
| Facility | The physical premises and the interior and exterior of a building(s). |
| HCC | HIPAA Compliance Committee. |
| HCWG | HIPAA Compliance Working Group. Group tasked with the county-level governance of the HIPAA Compliance Program. This includes corrective action, reviewing training and awareness needs, and other matters that impacts the county's compliance posture. Presents recommendations to the HCC and other respective county leadership. |
| HPO | HIPAA Privacy Officer. Individual tasked with the accountability to ensure privacy and security of PHI in all forms. Coordinates county HIPAA compliance governance activities, including day to day privacy matters impacting compliance, HIPAA events/incidents, and HCWG/HCC meetings. |
| HSO | HIPAA Security Officer. Individual tasked with the responsibility to ensure security of PHI in electronic form. Assists in coordinating county HIPAA compliance governance activities, including day to day security matters impacting compliance, HIPAA events/incidents, and HCWG/HCC meetings. |
| Health Care Component | Component of covered services provided by a hybrid entity under HIPAA. |
| HHS Office for Civil Rights | The OCR is responsible for enforcing HIPAA requirements, complaints, and violations. |
| HIPAA | Health Insurance Portability and Accountability Act of 1996 |
| HIPAA Breach Notification Rule | A set of federal standards (45 CFR §§ 164.400-414) that requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third-party service providers, pursuant to section 13407 of the HITECH Act. |
| HIPAA Event | An observable occurrence in an information system or process that warrants review by the HIPAA Working Group. |
| HIPAA Incident | A violation or immediate threat of violation of HIPAA Privacy and Security Rule policies, procedures, or standard county operating practice (e.g., OC Privacy Practices). |
| HIPAA Privacy Rule | A set of federal standards to protect the privacy of patients' medical records and other health information maintained by covered entities (health plans, which include many governmental health programs, such as the Veterans Health Administration, Medicare, and Medicaid; most doctors, hospitals and |

| | |
|---|---|
| | many other health care providers and health care clearinghouses) and by their business associates. |
| HIPAA Security Rule | A set of federal standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. The Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164. |
| HITECH | The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. |
| Hybrid Entity | A single legal entity:<br><br>(1) That is a covered entity;<br><br>(2) Whose business activities include both covered and non-covered functions; and<br><br>(3) That designates health care components in accordance with paragraph §164.105(a)(2)(iii)(D) of the Code of Federal Regulations. |
| Information Security | The act of protecting confidentiality, integrity, and availability of information. |
| Information System | An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. |
| Integrity | The property that data or information have not been altered or destroyed in an unauthorized manner. |
| Least Privilege | Principle of least privilege (POLP) is the practice of limiting access to the minimal level that will allow normal functioning. Applied to employees, the principle of least privilege translates to giving people the lowest level of user rights that they can have and still do their jobs. |
| Malicious Software | Software, for example, a virus, designed to damage or disrupt a system. |
| Minimally Necessary | A standard which means that people should only access, use or disclose the health information that is minimally necessary to accomplish a given task or purpose. |
| Mobile Computing Devices | A portable electronic device capable of recording, text, and voice communications, capturing images, and personal computing. This includes, but is not limited to: smart and cellular phones, laptops, tablets/slates, etc. |
| Multiple Authentication | A security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction. |
| Need to Know | The property, in the interest of securing PHI, has a requirement for access to, knowledge, or possession of the information to perform tasks essential to role. |
| The Notice | Oakland County Notice of Privacy Practices. |
| OC/County | Oakland County |
| Password | Confidential authentication information composed of a string of characters. |
| Person | Natural person, trust or estate, partnership, corporation, professional, association, or other entity, public or private |
| PHI | Protected health information means individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: |

| | |
|---|---|
| | (i) Transmitted by electronic media;<br><br>(ii) Maintained in electronic media; or<br><br>(iii) Transmitted or maintained in any other form or medium.<br><br>(2) Protected health information excludes individually identifiable health information:<br><br>(i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;<br><br>(ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);<br><br>(iii) In employment records held by a covered entity in its role as employer; and<br><br>(iv) Regarding a person who has been deceased for more than 50 years |
| Physical Safeguards | Physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion. |
| Policy | Principles, rules, and guidelines formulated or adopted by an organization to reach its long-term goals and typically published in a booklet or other form that is widely accessible. |
| Procedure | A fixed, step-by-step sequence of activities or course of action (with definite start and end points) that must be followed in the same order to correctly perform a task. It is the 'how' to implementing a policy. |
| Risk Analysis | The process of defining and analyzing the dangers to individuals, businesses and government agencies posed by potential natural and human-caused adverse events. |
| Risk Assessment | The process of identifying variables that have the potential to negatively impact an organization's ability to conduct business. |
| Risk Management | The process of identifying, assessing, and controlling threats to an organization's capital and earnings. These threats, or risks, could stem from a wide variety of sources, including financial uncertainty, legal liabilities, strategic management errors, accidents, and natural disasters. |
| Risk Mitigation | A systematic reduction in the extent of exposure to a risk and/or the likelihood of its occurrence. Also called risk reduction. |
| Safeguards | Control or security measure. See security measure definition. |
| Security Event | An observable occurrence in an information system or process that warrants review by Information Security. |
| Security Incident | A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. |
| Security Incident | An event that may indicate that an organization's systems or data have been compromised or that measures put in place to protect them have failed. |
| Security Measure | All administrative, physical, and technical safeguards in an information system. |
| Standard | Rule, condition, or requirement |
| Subcontractor | A subcontractor is an entity that creates, receives, maintains, or transmits protected health information on behalf of the business associate. |
| Technical Safeguards | Technology and related policies/procedures for its use that protect electronic protected health information and control access to it. |
| TPO | Treatment, payment, operations. |

| | |
|---|---|
| | Treatment, payment, or health care operations. (1) A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations.<br>(2) A covered entity may disclose protected health information for treatment activities of a health care provider.<br>(3) A covered entity may disclose protected health information to another covered entity or a health care provider for the payment activities of the entity that receives the information.<br>(4) A covered entity may disclose protected health information to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is:<br>(I) For a purpose listed in paragraph (1) or (2) of the definition of health care operations; or<br>(ii) For the purpose of health care fraud and abuse detection or compliance.<br>(5) A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to other participants in the organized health care arrangement for any health care operations activities of the organized health care arrangement. |
| Unsecured PHI | Protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons using a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5. |
| Use | With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information. |
| User | A person or entity with authorized access. |
| Vendor | An entity that provides technology products to the County. |
| Workforce Member | Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether they are paid by the covered entity or business associate. |
| Workstation | An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment. |