Oregon HISPC Project
General Privacy Standards – Version 3
February 21, 2007

The Oregon HISPC Team and stakeholders participating in the Oregon HISPC Project have identified the following effective and appropriate privacy standards as defined in the HIPAA Privacy Rule, Oregon law and what is considered by privacy professionals to be appropriate privacy standards. Some of the standards listed may be more stringent than HIPAA requirements. As with most states, Oregon continues its efforts to reasonably ensure such standards are uniformly followed by caretakers of individually identifiable health information (called protected health information or PHI under the HIPAA privacy rule).

The following privacy standards should be followed not only by HIPAA covered entities, but all entities with access to individually identifiable patient/health plan member data. This is especially true with the emergence on the market of personal health records maintained by "non-covered entities."

Healthcare Privacy Standards

State Law Preemption: A review of state statute preemptions versus HIPAA requirements needs to be developed or obtained. Appropriate policies, procedures and practices need to be implemented to reasonably ensure provisions of state law that preempt HIPAA are followed. This applies to PHI in any form (paper records, electronically stored records, verbal conversations, etc.). Members of a health information exchange network need to develop standards to isolate or mask specially protected health information from other participants in the exchange and implement policies and procedures that accommodate release of specially protected health information in a way that complies with state law, other federal law (such as 42 CFR Part 2) and accommodates timely health information exchange.

Compliance Reviews: Organizations involved in the health care industry (including entities not specifically covered by the HIPAA privacy rule) should be subject to periodic or random audits by designated state and federal bodies to reasonably ensure organizations are adhering to appropriate privacy practices. In the case of a health information exchange, member organizations need to be prepared to comply with any regulatorily defined audits by the state or federal government. This would include identifying a collaborative team or neutral third party to act as the liaison to the state or federal agency and provide whatever information is necessary regarding existing network privacy practices, enforcement of those practices, realized privacy breaches and related mitigation, etc.

Record Keeping & Access: State and federal law identify different retention periods for different types of data. As an example, HIPAA requires covered entities maintain records relating to compliance with the privacy rule for six years. Longer retention

periods may exist for certain classes of data (such as the medical record). Organizations are responsible to maintain defined categories of records for the periods of time defined in statute or rule. Also, organizations are required to make such records available to the regulatory body (federal or state) or the courts for the purpose of demonstrating appropriate record retention requirements and compliance with privacy rules governing the contents of records retained. Special attention needs to be paid to new federal electronic retention requirements released in December 2006.

Organizations involved in a health information exchange network are required to adhere to the same retention requirements and may elect to adhere to longer retention schedules where they deem it appropriate (such as efforts to maintain the continuity of a patient's record). In the event longer retention periods are agreed to, all participating organizations need adhere to the defined longer retention standards. Also, such organizations need to develop and enforce an appropriate data destruction process. There need to be reasonable assurances that data destruction occurs at the end of the retention period and destruction is done securely to reasonably ensure against inappropriate discloser or theft of PHI.

Healthcare Operations: Healthcare organizations that are considered HIPAA covered entities may exchange PHI for the purpose of healthcare operations without the patient/consumer's consent or written authorization (unless the PHI falls into a class of data that is additionally protected under state or federal law). Other organizations receiving, processing, storing, etc. individually identifiable health information should obtain authorization from the patient or consumer before release unless the release is governed by a HIPAA defined business associate agreement and used for treatment, payment or healthcare operations or if the health information had been de-identified before release. Healthcare operations includes quality assessment, case management, grievance resolution, underwriting, provider credentialing, contacting providers and patients regarding alternative treatment, developing web based applications that will be used for data dissemination to other organizations or patients/consumers, etc. Healthcare operations does not include research.

If the data is maintained as part of a health information network, common standards and definitions need to be documented that all organizations with access to the data are required to adhere to when using PHI for especially healthcare operations and also for treatment and payment.

Organized Health Care Arrangement (OCHA): Health care organizations that are HIPAA covered entities may enter into an agreement to operate under an umbrella arrangement that simplifies the process of recordkeeping, distribution of required documentation to the patient, etc. This means the covered entities entering into an organized health care arrangement must adopt the same privacy policies, procedures and practices, adopt a common or joint notice of privacy practices that is distributed to

patients and document the relationship between covered entities that make up the organized health care arrangement.

Similar practices should be established between non-covered entities that have access to identifiable healthcare information to allow simplification of business practices while continuing to protect the privacy of patients/consumers. Also, organizations involved in a health information exchange network need to develop common privacy policies, procedures and practices that are uniformly applied, uniformly communicated to patients/consumers and enforced across participating organizations.

Covered entities involved in a common data sharing network can take advantage of the benefits of an OCHA as long as policies, procedures and practices adopted adequately protect patient/consumer information and meet regulatory requirements (HIPAA, GLBA, Sarbanes Oxley, consumer protection laws, etc.).

Uses and Disclosures of Identifiable Health Information: An organization that is considered a HIPAA covered entity is permitted to disclose individually identifiable health information or PHI to an individual or entity for treatment, payment and healthcare operations without consent or authorization by the patient/consumer (unless the PHI falls into a class of data that is additionally protected under state or federal law). "Non-covered entity" organizations should obtain the authorization of the patient/consumer prior to releasing PHI for any reason unless the "non-covered entity" is operating as a business associate on behalf of a covered entity and such release is for treatment, payment or healthcare operations. Covered entities and "non-covered entity" organizations need to comply with more stringent state and federal statutes that require, in some instances, written consent or authorization from the patient/consumer or his or her personal representative prior to the initial release and, in some cases, before the data can be re-released.

Organizations participating in a healthcare information exchange network need to establish common practices related to the release of PHI for treatment, payment and healthcare operations. This includes provisions that address more stringent privacy requirements where consent or authorization is required of the patient/consumer.

Minimum Necessary: Organizations need to only disclose the minimum amount of PHI necessary to satisfy the reason for which the PHI is disclosed. This includes use of the PHI for intra or inter-organizational purposes. Minimum necessary does not apply to releases for treatment, when required by law, when disclosed to the OCR, disclosures for specific authorizations and when disclosed pursuant to provisions of the Privacy Rule to comply with the Privacy Rule. Even though such releases are exempt from the minimum necessary standard, it is appropriate to reasonably ensure, even for treatment, only the appropriate information is released. Safeguards need to be implemented and enforced that protect against disclosure of information that is specially

protected by statute or rule without specific consent or authorization from the patient/consumer or his or her personal representative.

Organizations who are members of a health information exchange are required to agree on and enforce practices that reasonably ensure only the data needed for a particular purpose is disclosed to members of the network and any other party that has access to the network. There should be an oversight body that consists of a collaborative team or neutral third party that regularly audits the exchange of and access to data to reasonably ensure minimum necessary standards are adhered to.

Release by Whistleblowers: Federal rule does allow for the release of individually identifiable information by workforce members (employees, temporaries, contractors and volunteers), business associates or members of a health information exchange network to a healthcare oversight agency or the privacy enforcement body if they believe the organization is unlawfully releasing or using PHI. While this is true, individual originations and network members need to specifically review such disclosures to reasonably ensure such disclosures meet the definition of whistleblower release. An individual or organization claiming whistleblower status while disclosing health information does not necessarily exempt the individual or organization from civil fines, tort, etc. if such a disclosure does not meet the whistleblower test.

Hybrid Entities: Hybrid entities (healthcare organizations with lines of business other than health plans, provider organizations or healthcare clearinghouses) need to reasonably ensure the health care components of the hybrid entity establishes appropriate barriers so PHI is not disclosed outside of the healthcare component of the organization. If a hybrid entity is a member of a health information exchange, the exchange should require the hybrid entity demonstrate that such safeguards are in place and enforced.

Affiliated Healthcare Organizations: Healthcare organizations may establish affiliate arrangements between organizations. If organizations affiliate formally, the affiliated organizations should establish formal agreements and establish similar or the same privacy policies, procedures and practices. If affiliated organizations participate in a health information exchange network, they should be required to demonstrate consistent application and enforcement of privacy policies, practices and procedures within the business relationship that is represented by the affiliation.

Business Associate Contracts: Any healthcare organization, whether or not it is required to comply with the HIPAA Privacy Rule, should enter into formal contracts with business associates (third parties with access to individually identifiable information working on behalf of the healthcare organization) clearly defining what the business associate's relationship is with the healthcare organization and what PHI is to be exchanged between the healthcare organization and the business associate. The business

associate contract needs to require the business associate adhere to the requirements of the Privacy Rule and appropriate privacy practices. Healthcare organizations should reasonably ensure business associates adhere to the provisions of the Privacy Rule and appropriate privacy practices.

Healthcare organizations are not required to audit business associates from a regulatory perspective but from a sound privacy practice perspective, the healthcare organization should make a reasonable effort to reasonably ensure the business associate has adopted appropriate privacy policies, procedures and practices and is enforcing them. Also, covered entities are required under the HIPAA privacy rule to terminate a contract with a business associate if they breach the business associate contract or, if contract termination is not possible, work with the business associate to mitigate damages and report the breach to the Office of Civil Rights (OCR), US Department of Health and Human Services (HHS). Non-covered entities should also follow the same practice (except for the requirement to report the breach to OCR).

Prior to formation of a health information exchange network, participating organizations should develop a common business associate contract that specifically addresses privacy requirements for any third party with access to individually identifiable health information on behalf of the network and network members. Also, member organizations should not allow third parties to access the network without specific approval of network members or a designated governing body. Guidelines/requirements when such access will be allowed needs to be clearly defined and enforced.

Group Health Plans: Healthcare organizations (covered entities or "non-covered entities") should disclose only the minimum amount of individually identifiable health information (IIHI, PHI) necessary to assist in group health plan practices. The group health plan document needs to clearly state when and what PHI is disclosed and for what purpose. The group health plan, as specified in the plan document, needs to reasonably ensure appropriate safeguards are in place so PHI is not disclosed outside of the group health plan. This means that business operations, especially those involving the use and disclosure of PHI need to be "walled off" or segregated from the rest of the business operation, allowing only "health plan" employees access to PHI.

If members of the group health plan's workforce are allowed access to a health information exchange network for payment or healthcare operations, required privacy practices need to be defined and communicated to the group health plan and adopted by the group health plan prior to allowing the group health plan's workforce members access to the network. Network functionality needs to include the ability to enforce minimum necessary access. Also, access by outside parties such as group health plans should be audited by a collaborative team or neutral third party on a regular basis.

Release Without Consent or Authorization: A healthcare organization that is a HIPAA covered entity is allowed to release PHI without consent or authorization for the following purposes:

- To a public health authority
- To a public authority for child abuse or neglect reasons (subject to state law requirements)
- If the person is subject to the Food and Drug Administration (FDA) for the purpose of tracking recalls of prescription medication, reporting adverse events resulting from certain forms of treatment, etc.
- If an individual presents for treatment of a communicable disease
- Such a report of a medical incident is related to a workforce incident

Any such release needs to meet minimum necessary standards. Appropriate policies, procedures and practices should be implemented to reasonably ensure data released for any of the above purposes meets minimum necessary standards. Also, such release without consent or authorization is considered a disclosure that needs to be tracked and communicated to the patient/consumer if the patient/consumer so requests.

A healthcare organization may also disclose PHI in the event of a disaster to assist in disaster relief. Such disclosures for assistance in disaster relief need to adhere to minimum necessary standards and be recorded as a disclosure to be included in any future accounting for disclosures.

"Non-covered" healthcare organizations should obtain patient/consumer consent or authorization prior to releasing IIHI for the above purposes unless the "non-covered" healthcare organization is a business associate of a covered entity and the appropriate business associate contract has been executed.

When a health information exchange network is formed, all member organizations need to adhere to the above standards and make available to all members a list of such disclosures. When a member organization is required to send an accounting of disclosures to the patient/consumer, disclosure of network data for the above reasons needs to be included in the accounting of disclosures.

Release for Abuse, Neglect or Domestic Violence: A healthcare organization is permitted to disclose PHI in the event child abuse, neglect or domestic violence is suspected to the appropriate regulatory entity and as defined under state law. Unless otherwise noted in statute or rule, such disclosures need to be included in any accounting of disclosures. Also, HIPAA requires the individual who is reported to the appropriate authorities because of suspected abuse, neglect or domestic violence is immediately notified that a report has been made unless:

- Notification could cause harm to the individual

- If the person reported is the personal representative of the patient/consumer and the personal representative is the individual is the suspected or known perpetrator

Healthcare or Consumer Protection Oversight Activities: Organizations who are HIPAA covered entities are authorized to release PHI for healthcare oversight activities to:

- The healthcare system
- Government benefit programs
- Entities subject to government oversight activities
- Entities subject to civil laws where such release is necessary to determine compliance with said civil laws

"Non-covered" healthcare organizations may also be subject to similar release requirements if so defined in statute or rule (federal or state). This would include release for consumer protection purposes. Such disclosures need to be accounted for and included in any accounting of disclosures made to the patient/consumer. All disclosures for the above purposes need to follow minimum necessary requirements.

If a release for the above purposes is made by a member of a health information exchange network from a commonly accessible health information, the same requirements apply as those listed under "Release Without Consent or Authorization."

Judicial and Administrative Proceedings: Healthcare organizations may release PHI for judicial and administrative proceedings when court documents specifically authorize such release. Also, release may be made pursuant to a duly authorized subpoena. The healthcare organization is required to ascertain that the individual whose PHI is to be released has been properly notified or attempts have been made to notify the individual. Minimum necessary requirements apply and such disclosures need to be accounted for and included in any accounting of disclosures.

If such disclosures are made from common data stored on a health information exchange network, policies, procedures and practices need to be implemented to determine if the request for release is valid, reasonably ensure efforts are made to notify the patient/consumer or personal representative, minimum necessary standards are followed and the disclosure is accounted for on the network in a location accessible to all member organizations.

Release for Law Enforcement Activities: Healthcare organizations who are HIPAA covered entities may release PHI to law enforcement authorities in identifying certain wounds or related injuries. Also, a covered entity may release PHI to law enforcement authorities to assist in locating fugitives. The covered entity needs to review such releases for minimum necessary requirements and to determine if de-identified data would not serve the required purpose. This does not represent a general release and, unless specifically required by law (federal or state), such disclosures are not

permissible without patient/consumer or personal representative consent or authorization.

"Non-covered" entities should not disclose information to law enforcement without the appropriate authorization from the courts or as defined in statute or rule (federal or state). If these conditions are not met, the "non-covered" entity should not release information to law enforcement without specific authorization from the patient/consumer or personal representative.

If such disclosures are made of common data stored on a health information exchange network, policies, procedures and practices need to be implemented to determine if the request for release is valid as defined under statute and rule (federal and state), determine if de-identified information could be disclosed rather than PHI, minimum necessary standards are followed and the disclosure is accounted for on the network in a location accessible to all member organizations.

Release of PHI for Research without Authorization: PHI may be released for research purposes without authorization of the individual if such is approved by an Institutional Review Board prior to release of PHI. This is only true for healthcare organizations that are HIPAA covered entities and when not prohibited by state law. "Non-covered" entities should obtain the authorization from the patient/consumer or personal representative prior to using any identifiable information for research or research related purposes.

Use of PHI stored on a health information exchange network for research purposes needs to be fully defined and agreed to by all member organizations. Unless a common IRB is formed, any release for research requires specific authorization from the patient/consumer or personal representative.

Avert a Serious Threat to Safety: A healthcare organization may release PHI in the event, in the professional judgment of the healthcare organization, such release will prevent a serious threat to public safety or to the safety of another. Any such disclosure needs to follow minimum necessary requirements and be accounted for as a disclosure to be included in any future accounting of disclosures.

Disclosure for Specialized Government Functions: A healthcare organization that is a HIPAA covered entity may release PHI for the following purposes:

- Military activity
- National security or intelligence activity
- Protective services for the President and others
- Medical suitability determinations (Department of State)
- Correctional institutions or law enforcement custodial situations
- Covered entities that are governmental programs providing public benefits

Any "non-covered" entity should only release PHI for the purposes described above if specifically required by statute or rule (federal or state) or with specific authorization from the patient/consumer or personal representative. Covered entities and "non-covered" entities need to follow minimum necessary standards and account for such disclosures unless specifically prohibited by statute or rule (state or federal).

If such disclosures are made of common data stored on a health information exchange network, policies, procedures and practices need to be implemented to determine if the request for release is valid as defined under statute and rule (federal and state), minimum necessary standards are followed and the disclosure is accounted for in a location accessible to all member organizations unless accounting for later use in accounting of disclosures is specifically prohibited by state or federal statute or rule.

Workers Compensation: Healthcare organizations may disclose PHI to workers compensation programs for the purpose of meeting workers compensation activities. Workers compensation is specifically exempted from coverage under the Privacy Rule. Such disclosures need to meet minimum necessary requirements and need to be recorded as a disclosure for use in any future accounting of disclosures.

Marketing: A healthcare organization that is a HIPAA covered entity is prohibited from using PHI for marketing purposes unless the organization obtains appropriate authorization from the patient/consumer. A covered entity may market to a patient/consumer under the following circumstances:

- Such marketing occurs in a face-to-face encounter with the patient/consumer
- The product or service to be marketed is of nominal value
- Covers health related products or services of the covered entity or an affiliated third party and such marketing communication meets the HIPAA requirements

The organization may release PHI for marketing to its business associate if such release is for approved marketing to a patient/consumer. An exception to the prohibition to market to patient/consumer without authorization is marketing to a broad group through a newsletter unless said newsletter targets a specific condition and the newsletter is not mailed in a security envelope.

"Non-covered" entities should not use IIHI to market to patients/consumers unless specifically authorized by the patient/consumer in advance. Any marketing that clearly identifies a condition (especially if the condition is considered specially protected under state or federal statute), needs to be done in such a way as the marketing material identifying the condition is not visible until the envelope or package is opened by the recipient.

Specific marketing rules need to be developed, agreed on and enforced by organizations who are members of a health information exchange where commonly

held data may be used for marketing purposes. While not specifically required, all marketing by the exchange should not occur without the specific consent of the patient/consumer.

Fund Raising: A healthcare organization may use certain PHI for fund raising purposes. That information includes:

- Demographic information about the patient/consumer
- Date(s) healthcare services were provided

The healthcare organization must provide an opt out opportunity for individuals fund raising material is sent to and must make every effort to reasonably ensure the patient/consumer opting out no longer receives any fund raising material. This is true for covered entities, "non-covered" entities and health information exchange networks.

Underwriting: Any health plan receiving PHI for the purpose of underwriting, premium setting or activities related to establishing a contract may not further disclose the PHI unless required by law.

Verification: Healthcare organizations must make a reasonable effort to verify the validity of a disclosure of PHI before the PHI is disclosed to another healthcare organization or third party. This means obtaining documents, statements or representations (oral or written) from the party the PHI will be disclosed to verifying their authority to receive such PHI or authenticating the third party using a commonly developed authentication database. This includes verifying the authority of public entities requesting disclosure of PHI which may consist of presenting a badge, presenting a document on official government stationary, etc. It also may include presentation by the requestor of a signed authorization when the release includes specially protected health information.

Specific authentication criteria need to be developed and agreed to by all organizations participating in a health information exchange network. Authentication requirements need to be strictly followed by all member organizations and members of their workforce. Also, following proper authentication policies, procedures and practices by member organizations and members of their workforce need to be audited on a regular basis to reasonably ensure appropriate authentication occurs prior to release of PHI and minimum necessary standards are met.

Privacy Official: All healthcare organizations must appoint a privacy official who is responsible for overseeing the organizations' privacy program, compliance with applicable statute and rule (federal and state) and compliance with appropriate privacy practices. A neutral privacy official or collaborative privacy team needs to be established when forming a health information exchange network and be responsible for privacy program oversight as it applies to the network.

Staff Training: Healthcare organizations must provide privacy training to the workforce. The workforce includes employees, temporaries, volunteers and contracted employees. This is true for HIPAA covered entities, "non-covered" entities and members of health information exchange networks.

Standard Safeguards: Healthcare organizations must implement policies, procedures and practices that reasonably ensure administrative, technical and physical security of PHI. This includes PHI in any form (e.g., electronic, voice, written, images, etc.). This is true for HIPAA covered entities, "non-covered" entities and members of health information exchange networks.

Sanctions: Healthcare organizations must provide for workforce sanctions in the event the applicable regulations or the healthcare organizations' privacy policies, procedures or practices are violated. This is true for HIPAA covered entities, "non-covered" entities and members of health information exchange networks. Sanctions need to be developed and enforced equally across all members of a health information exchange. This could include a written warning up to termination of exchange access,

Mitigation: Healthcare organizations are required to take all reasonable action to mitigate damages in the event PHI is inadvertently or inappropriately released. This is true for HIPAA covered entities, "non-covered" entities and members of health information exchange networks. Also, any inappropriate disclosure needs to be tracked and included in any future accounting of disclosures.

Privacy Policies & Procedures: Healthcare organizations should develop and implement privacy policies and procedures that fully implement requirements of any applicable statute or regulation (state or federal) and appropriate privacy practices. Healthcare organizations should periodically review and update privacy policies and procedures to accommodate changes in business practices and changes in law. Healthcare organizations should also update and distribute their notice of privacy practices if changes in policy and procedure materially impact the provisions of the notice. This is true for HIPAA covered entities, "non-covered" entities and members of health information exchange networks.

Changes to privacy policies, procedures and practices need to be clearly communicated to members of the workforce, third party business associates and all members of a health information exchange network as well as members of their workforce. When any changes are made, the prior version of the policy, procedure or practice should be maintained for period of not less than six years from the date the policy, procedure or practice was in effect.

Healthcare Privacy Standards – Consumer/Patient Rights

Consumer/Patient Complaints to the Organization and Other Appropriate Authorities: Organizations need to allow consumers/patients the ability to file complaints with the organization and with appropriate designated governmental entities (for HIPAA the appropriate authority is the Secretary of HHS, delegated to OCR and for the Gram-Leach-Bliley Act (GLBA), the Insurance Division, Oregon Department of Consumer and Business Services) regarding non-compliance with the privacy regulations/statute and sound privacy practices.

Requests for Restrictions on Disclosure: Healthcare organizations need to allow patient/consumers the opportunity to request partial or complete PHI access restrictions to their medical record. Such restriction requests should be honored where feasible. If the healthcare organization agrees to any restrictions, the healthcare organization is responsible for reasonably ensuring agreed upon restrictions are adhered to. If members of a health information exchange network agree to allow restrictions to commonly held data, appropriate procedures need to be implemented to reasonably ensure restriction requests that are granted are adhered to. Also, all member organizations should agree to the same restriction policy. If restriction requests are accommodated by some but not all participating organizations, data integrity and record completeness become an issue.

Disclosure of De-identified Information: There are no restrictions regarding the release properly of de-identified PHI. De-identified data means data that a reasonable person would be unable to re-identify to an individual and is specifically defined in the HIPAA privacy rule.

Release of PHI for Deceased Individuals: Healthcare organizations must adhere to minimum necessary requirements when releasing PHI about deceased individuals.

Release of PHI to Personal Representatives: Healthcare organizations must treat personal representatives in the same manner as the patient/consumer. The healthcare organization may elect not to recognize a designated personal representative as the personal representative for the purposes of releasing PHI if the healthcare organization suspects abuse, domestic violence or neglect of the patent/consumer by the personal representative.

Consent: Healthcare organizations who are HIPAA covered entities are not required to obtain a patient/consumer's consent prior to sharing PHI for treatment, payment or healthcare operations (except as specified under state and federal statute and rule). "Nov-covered" entities should require the consent of the patient/consumer when release is for healthcare operations. Healthcare organizations may require the patient/consumer sign a consent form (not the same as consent to treat; this refers to consent to release or share PHI) prior to providing treatment or enrollment in a health plan especially if

treatment information is specifically protected and requires patient/consumer consent prior to subsequent release (even for billing purposes).

If the healthcare organization requires patient/consumer consent, the healthcare organization is required to inform the individual in plain language the purpose of consent, the right of the individual to request a restriction to release of PHI, that a healthcare organization is not required to honor requests for restriction of release and that such restrictions, if honored, may be revoked upon notice to the patient/consumer.

Authorization Requirements: Unless specifically allowed pursuant to applicable statute or rule (state or federal), disclosures of PHI is not allowed without specific authorization of the patient/consumer. This includes release by HIPAA covered organizations and non-covered organizations. A valid authorization needs to be specific and time or event limited. Authorizations are required for the use of PHI for research purposes with limited exceptions. A healthcare organization may not condition treatment or enrollment in a health plan on providing authorization unless treatment is conditional on participating in the research project. Authorizations may be revoked by the patient/consumer at any time but such revocation does not apply to the exchange of PHI prior to such revocation.

Standard authorization policies, procedures, practices and forms need to be developed and agreed to by all organizations participating in a health information exchange network. This includes development of a common authorization form, adherence to minimum necessary standards and retention of the authorization form for a minimum of six years.

Allowance for a Patient/Consumer to Object to Release of PHI: A patient/consumer has the right to object to publication of their PHI in a facility directory. The patient/consumer also should be allowed the opportunity to object to the release of PHI to friends and family prior to such release. The right to object does not need to be in writing. In the event of an emergency when a patient/consumer is unable to exercise his/her right to object to release, the healthcare organization has the authority to release a patient/consumer's PHI to friends, family, clergy, and list such information in the facility directory if such release is deemed in the best interest of the patient/consumer or deemed necessary to provide appropriate patient/consumer medical care.

Notice of Privacy Practices: A healthcare provider or other healthcare organization with direct contact with the patient/consumer must provide a copy of the organization's notice of privacy practices to the patient/consumer during first encounter and make every effort to obtain written verification from the patient/consumer that the notice of privacy practices was presented to the patient/consumer. This would include any organizations marketing and/or maintaining a personal health record. Health plans are required to mail notices of privacy practices to participating members. Health plans are

not required to obtain written verification from members that they received a copy of the notice. Healthcare organizations are required notify patients/consumers if significant changes are made to the notice. All notices should be clearly understandable by the patient/consumer and a member of the workforce should be available to provide the patient/consumer with any needed clarification.

Healthcare organizations are required to notify patients/consumers once every three years of the availability of the notice. Notification may be through a newsletter or other mailing to the patient/consumer, face-to-face, etc. If the healthcare organization is required to adhere to GLBA (primarily health planls), the organization is required to mail a current version of the organization's notice of privacy practices to patients/consumers annually. If the healthcare organization maintains a web site, the notice should be prominently posted on the web site. Healthcare organizations participating in an organized health care arrangement may issue a joint notice of privacy practices.

Organizations participating in a health information exchange network need to include language about such participation to patients/consumers through the organization's notice. Such language should be standard and consistent across all members of the network.

Confidential Communications: Healthcare organizations should accommodate any reasonable requests for alternate forms of communication with a patient/consumer.

Access to Protected Health Information: Healthcare organizations must allow a patient/consumer access to their protected health information contained in their designated record set except for:

- Psychotherapy notes
- Information collected in preparation for a civil or criminal proceeding
- Information specifically identified under CLIA or specifically exempted from CLIA (laboratory results)

Healthcare organizations may deny access to the following information and it is not reviewable or appealable by the patient/consumer:

- Access is deniable pursuant to the preceding list
- PHI is generated by a correctional institution or on behalf of the correctional institution
- PHI is collected for research purposes and the individually previously agreed to a denial of access while the research is being conducted
- Such PHI is protected by the Privacy Act
- Information is provided by a third party where a request for the protection of confidentiality of release was granted

The individual has the right to appeal to a qualified medical professional the denial of release of PHI that is not disclosed for the following purposes:

- An authorized healthcare professional has determined that such release, to an individual or a personal healthcare representative, would be harmful to the individual or others
- The PHI makes reference to another individual

The healthcare organization should provide the patient/consumer access to the designated record set within 30 days (this time frame is required for HIPAA covered entities and should be adhered to by "non-covered" entities). The time line for release of information may be extended for up to 60 days if the records are not readily available as long as the patient/consumer is informed within the initial 30 day period.

The healthcare organization must make the designated record set available for review for free but may charge a reasonable fee for copies of the designated record set (a limit of charges may be set in state statute). If the healthcare organization denies the patient/consumer access to part of his or her designated record set, the healthcare organization must notify the patient/consumer in writing and inform the patient/consumer if he or she has a right of appeal and, if so, how to appeal the denial decision.

When a health information exchange network is formed, member organizations should define a common designated record set, processes and forms for requesting to review or for a copy of the designated record set, appeal processes, etc. prior to creating a common data set. All participating members should be required to adhere to the established designated record set definition and related policies, procedures and practices.

Amendment to PHI: Healthcare organizations must allow a patient/consumer the opportunity to request an amendment to his or her designated record set. The healthcare organization is not required to honor any requests for amendment and has a responsibility to inform the patient/consumer if a request for amendment is denied or partially denied. The healthcare organization should inform the patient/consumer the reason for any denial or partial denial and provide any associated documentation to support the denial.(e.g., a statement, "The record is correct," is not a sufficient explanation of why an amendment was denied or partially denied) (this is required for all HIPAA covered entities). If the request for amendment is denied, the patient/consumer has the right to submit a rebuttal and request a copy of his or her request for amendment and rebuttal be included in his or her designated record set and be included when that portion of the record is shared with any other entity. The healthcare organization may include a response to the patient/consumer's rebuttal if desired.

If the healthcare organization approves or partially approves the request for amendment, the healthcare organization is responsible for informing the patient/consumer. The healthcare organization is responsible for providing the patient/consumer a copy of the amended record. Also, the healthcare organization has

a responsibility to distribute a copy of the amended record to any other entity the healthcare organization has shared that portion of the record with.

Organizations who are members of a health information exchange network need to develop common policies, procedures and practices that reasonably ensure the patient/consumer's right to request an amendment is enforced, the handling of any amendment, denial of amendment, etc. is handled consistently and that the record amendment and possible denial or partial denial information becomes a permanent part of the medical record.

Accounting of Disclosures: Healthcare organizations must make available to the patient/consumer an accounting of disclosures of PHI if such a disclosure is made for purposes other than treatment, payment, healthcare operations or specifically authorized by the patient/consumer. This includes accounting for inadvertent or inappropriate disclosures of PHI but does not include accounting for incidental disclosures of PHI. Such a record must be maintained for six years. The healthcare organization should provide an accounting of disclosures within 60 days (HIPAA covered entities are required to adhere to this time frame) if requested by a patient/consumer. This includes only qualifying disclosures made on or after April 14, 2003, the effective date of the HIPAA Privacy Rule (while this standard should apply to "non-covered" entities, the Privacy Rule effective date may serve as a starting point for maintaining a record of disclosures).

Members of a health information exchange network need to develop commonly agreed to standards regarding the provision of an accounting of disclosures for commonly held data (versus data held at the provider level). Patients/consumers are entitled to notice, if they request it, of disclosures made by the network including unauthorized disclosures.

Waiver of Rights: Healthcare organizations that are HIPAA covered entities are prohibited from requiring a patient/consumer waive his or her rights under the Privacy Rule as a condition of treatment, payment, healthcare operations or enrollment in a health plan. "Non-covered" entities should also follow the same principle and not require a patient/consumer waive his or her right to privacy or rights as defined by appropriate regulation or appropriate privacy practices as a condition of interacting with or participating in any program where IIHI is collected, stored, transmitted, etc.

Notice of Inappropriate Release of PHI: Healthcare organizations should promptly notify any patient/consumer when his or her PHI is inappropriately released. Also, in the event of inappropriate release, the healthcare organization has a responsibility to take all reasonable measures to mitigate the damage to the patient/consumer and the organization. This includes changing policies, procedures or practices to reasonably ensure such an inappropriate disclosure does not occur in the future.