



Get HMIS.INFOrmed!

# Implementing an HMIS within HIPAA



Jon Neiditz

Atlanta, GA

(678) 427-7809

[jneiditz@hunton.com](mailto:jneiditz@hunton.com)



National HMIS Conference  
September 14th and 15th, 2004  
Chicago, IL

Sponsored by the U.S. Department of Housing and Urban Development



# HIPAA and HMIS Implementation

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) creates challenges for HMIS implementations that are unintended consequences
  - Many arise from failure of HIPAA to contemplate continuums of care (CoCs)
- The new HMIS standards do not address those challenges, but rather defer to HIPAA standards
- Therefore, careful structuring of HMIS arrangements will be necessary to accommodate HIPAA
- However, many homeless organizations (CHOs) need be governed by HIPAA less than they think

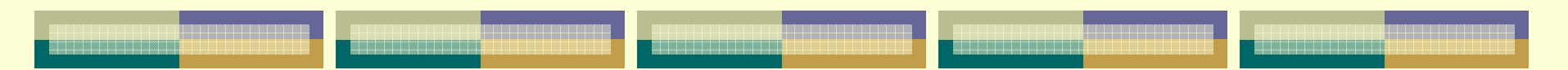


# HIPAA: Limited Jurisdiction

The only ways in which an entity becomes regulated under HIPAA is if it is

- (a) a “health care provider” that engages in one of HIPAA’s covered standard transactions electronically,
- (b) a “clearinghouse” or
- (c) a “health plan.”[\[1\]](#)

[\[1\]](#) 45 CFR 160.102



# Neither a CoC nor an HMIS is a “Clearinghouse”

*A clearinghouse* is defined by HIPAA as:

a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and “value-added” networks and switches, that does either of the following functions:

- (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
- (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.[\[1\]](#)

[\[1\]](#) 45 CFR 160.103



# COCs that Provide Health Care Are Often Not HIPAA-Covered Providers

Even if a CHO is *health care provider* for HIPAA purposes, it may not be a health care provider covered by HIPAA. If you are a CHO and are not sure whether you are a *health care provider*, you may not need to spend time and/or money finding out, because the only way HIPAA regulations cover you is if you are BOTH a *health care provider* and engage in covered standard transactions electronically. What, then, are these transactions?

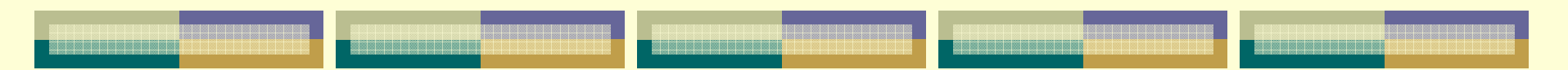
# HIPAA's Standard Transactions

## **Standard transactions are defined for the following:**

- Health claims or equivalent encounter (X12N 837)
- Retail pharmacy claims (NCPDP Version 5.1)
- Enrollment and disenrollment in a health plan (X12 834)
- Eligibility for health plan - inquiry/response (X12N 270-271)
- Healthcare payment and remittance advice (X12N 835)
- Health claim status - inquiry/response (X12N 276-277)
- Coordination of benefits (X12N 837)
- Referral certification (X12N 278)
- Referral authorization (X12N 278)
- Health plan premiums (X12 820)

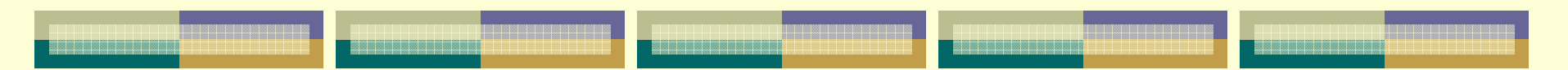
## **No rules have been issued for these transactions:**

- First report of injury
- Health claims attachments



# Even CHOs that Are HIPAA-Covered Providers Can Be “Hybrid Entities”

- HIPAA allows flexible structuring of covered providers as “hybrids” with covered and non-covered components.
- A CHO’s non-covered functions (for example, intake that may triage to covered and non-covered services) may be defined as a non-covered components of a hybrid entity exempt from HIPAA’s rules.
- The trade-offs in choosing a hybrid entity structure often balance information flow within the CHO against subjecting non-covered functions to rules poorly-designed to meet client and CHO needs.



# Let's Say That You have a Clinic Billing Medicaid...

- Consider structuring yourself as a “hybrid entity.”
- Information from the “covered components” will be subject to the HIPAA rules (and state confidentiality rules more protective than HIPAA).
- Information from the noncovered components will be subject to the HMIS standards (and state confidentiality rules more protective than the HMIS standards).
- “Firewalls” will need to be erected between covered and noncovered components.



# The Logic of HIPAA Uses and Disclosures

1. Must be a legal basis for a use or disclosure
  - Treatment, payment, health care operations
  - Authorization
  - Required by law, public health, judicial, research, etc.
  - Opportunity to agree or object
2. “Minimum necessary” requirement
3. Verification
  - Identity
  - Authority



# Treatment, Payment or Operations

- **Legal basis # 1:** Uses/disclosures of protected health information (PHI) relating to **treatment, payment or health care operations (TPO)**
  - **Treatment** of a patient (referral, admission, consultation, diagnosis, treatment planning – excludes “psychotherapy notes”)
  - **Payment** for services to a patient (billing, remittance, utilization review, medical necessity)
  - **Healthcare operations** – administrative processes using PHI (e.g. quality improvement, peer review/credentialing, training programs, medical/legal reviews, compliance, fraud and abuse, business planning, complaints and grievances)
- HIPAA didn't think enough about CoCs



# Governmental, Legal, Research Purposes (45 CFR 164.512)

- **Legal Basis # 2: Authorization not required** for certain disclosures to government agencies or legal processes
  - Uses and disclosures required by law
  - Public health, health oversight and regulatory agency activities
  - Cases of neglect, abuse or domestic violence
  - Judicial and administrative proceedings
  - Law enforcement investigations
  - Deceased individuals and organ donors
  - Serious threats to health or safety
  - Workers' compensation
  - Disclosure of “de-identified” health information
  - Research (differently defined than in HMIS rules)



# With Opportunity to Agree or Object

- **Legal Basis # 3:** For certain disclosures, we first must give the member an **opportunity to agree or object**, when possible
  - Limited information for use in facility directories
  - Coordination with disaster relief services
  - Disclosure to law enforcement regarding victim of a crime
  - Limited disclosure to family members for ongoing care

# With Written Authorization

- **Legal Basis # 4: Any use or disclosure not satisfying #1, #2 or #3 may be made only with the member's written authorization**
- **HIPAA Authorizations Must Contain:**
  - Meaningful and specific description of information
  - Persons authorized to disclose
  - Persons to whom disclosure may be made
  - Right to revoke
  - Information subject to re-disclosure
  - Expiration date
- **Compare HMIS Implied and Oral Consents:**
  - "Consent of the individual for data collection may be inferred from the circumstances of the collection."
  - CHOs MAY require either oral or written consents of themselves.



# Step 2: Minimum Necessary Standard

## Minimum Necessary Use and Disclosure (MND)

### ● General rule:

- Take reasonable measures to use or disclose only the minimum amount of information needed to accomplish intended purpose
- For routine uses and disclosures, based on “**need to know**”
  - **For disclosures**, protocols provide guidance on information that can be provided in common situations
  - **For uses**, access is based on minimum information needed to perform job functions
- For other disclosures, MND is determined on a case by case basis by the Privacy Officer using written criteria



# Minimum Necessary Standard Continued

## Minimum Necessary Disclosure (MND)

### ● Other rules

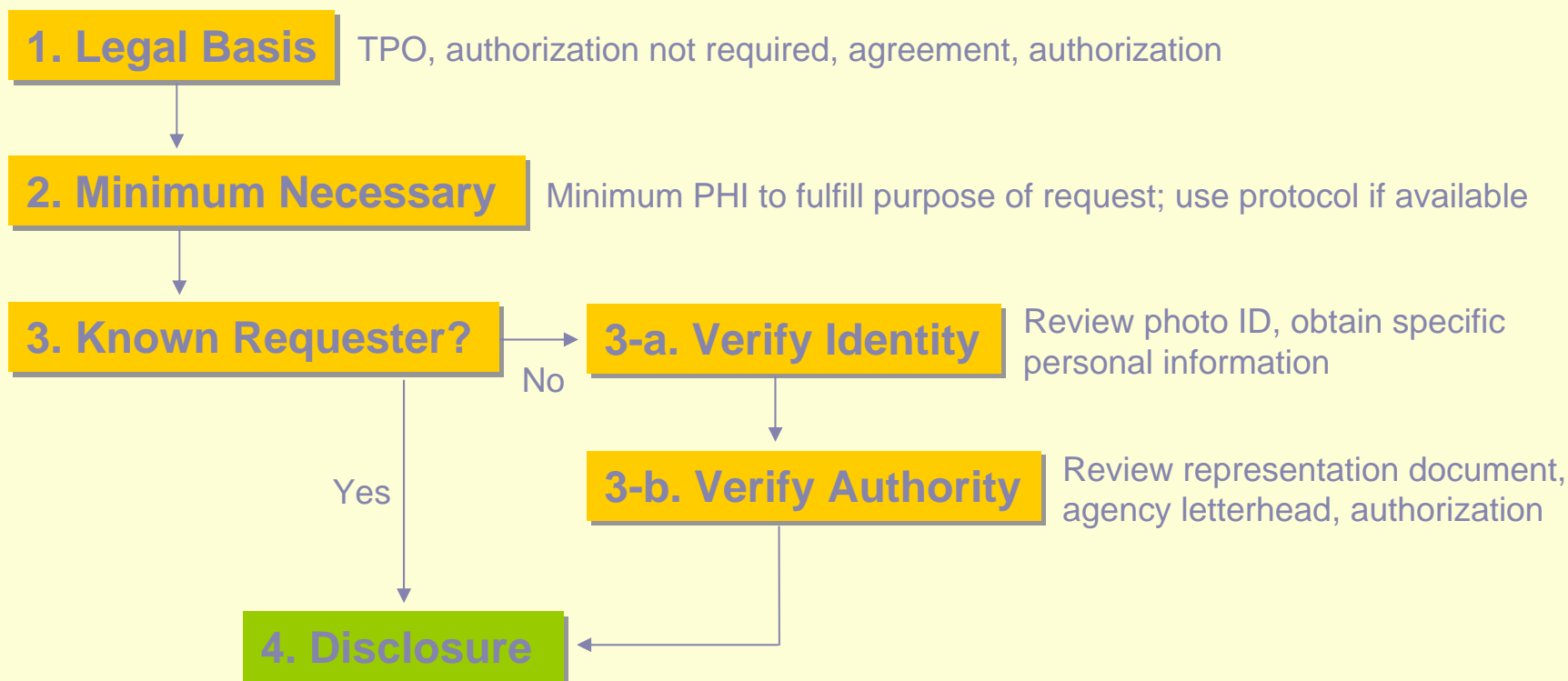
- When one covered entity request PHI from another covered entity, the requesting covered entity determines the minimum amount of PHI needed in its disclosure request
- MND does not apply to disclosures:
  - To a provider for treatment
  - To the individual
  - Made with an authorization
  - Required by law



## Step 3: Verification of Identity & Authority

- Reasonable efforts to verify the identity and authority of a requestor to receive PHI, if not known
- Establish identity through a combination of personal information elements, which differ if in person, by phone or by fax
- Establish authority by reviewing documentation or patient relationship:
  - Status as parent (or custodial parent following divorce)
  - Is the requester the patient's legal representative?
    - Named in a durable power of attorney for health care
    - Named in an appointment of representative letter
    - Appointed guardian by a court order
    - Named in an advance directive
  - Does the requester have written authorization from the patient?

# HIPAA Use and Disclosure Algorithm



# HMIS Disclosure Algorithm (Baseline)

## 1. Appropriate Purpose or Legal Requirement

### Requirement

administrative functions, deidentification, required by law, to avert a serious threat to health or safety, about victims of abuse, neglect or domestic violence, academic research purposes (with no HIPAA-like rules), law enforcement purposes. (Not an exhaustive list.)

Provide or coordinate services, payment or reimbursement,

## 2. Relevant to the Purpose to Be Used

Accurate, complete, timely

## 3. Known Requester?

No

## 3-a. Verify Identity

Review photo ID, obtain specific personal information

Yes

## 4. Disclosure

(Important missing step: verification of authority?)



# HIPAA, HMIS, State Law and Other Federal Law

- Both HIPAA and the HMIS standards defer to state laws that are more “stringent” -- more protective of privacy -- than the federal standards
  - State AIDS, mental health and substance abuse confidentiality laws are often more stringent than HIPAA
  - State medical records disclosure laws often do not defer to HIPAA’s concept of “TPO”
  - State laws less stringent than HIPAA but more stringent than the baseline HMIS standards govern non-HIPAA-covered CoCs and CHOs
- CoCs and CHOs are also often subject to the federal substance abuse record confidentiality rules, 42 CFR Part 2



# Is the CoC or HMIS a Business Associate of Participating Covered Entities?

- HIPAA's Definition of Business Associate (two-part test):
  - A contractor that receives PHI from a covered entity, its business associate or an organized health care arrangement
  - For the purpose of assisting with or performing a function **for or on behalf of** that covered entity (or organized health care arrangement)
- Business Associate (BA) relationship exists when the BA performs a function that the covered entity could perform for itself. Guideline:
  - Includes: administrative, management, financial functions
  - Generally excludes: services requiring licensure; but note that legal and accounting services are BA services
- BA status
  - Unlike covered entity status, BA status is relative
  - Determined by context of relationship with each covered entity



# What Business Associates are Not

- Business associates are not subject to HIPAA or HHS regulation
  - Not required to, e.g., have a privacy officer, produce notice of privacy practices, have written policies and procedures, obtain authorization or consents, have a complaint system, or institute “firewalls” between covered and non-covered functions (as is done by hybrid entities)
- Instead, requirements and specific obligations are set by the covered entity based on regulations and their own discretion
- Will vary according to covered entity/client, depending on functions performed by the business associate, risks, degree of oversight desired, and contractual protections desired



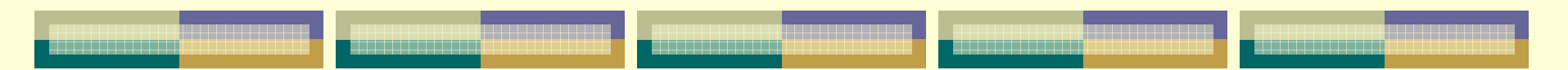
# Liability Standards and Implications

- Covered Entity (CE) only held responsible by HHS for conduct of BA if:
  - the CE knew of a pattern of behavior by the BA that constitutes a material breach of the BA agreement; and
  - the covered entity failed to take appropriate action
- Implications:
  - The CE is responsible for getting the BA's assurances (which are recorded in the BA agreement) but not for conducting oversight of the BA
  - Even if a CoC can use PHI in ways that may be dangerous to the CE, the CE is not likely to have the resources to monitor the CoC



# Business Associate Agreements

- Business associate agreement must contain at least certain provisions that address specific issues [164.504(e)]:
  - Permitted uses and disclosures of PHI
  - Appropriate safeguards of records
  - Report any unauthorized disclosures to entity
  - Subcontractors must agree to same conditions and restrictions
  - Make PHI available for inspection, amendment, accounting
  - Make books and records available for inspection by DHHS
  - Destroy/return PHI at termination of contract
  - Material breach by associate is grounds for termination



# Security Rule Requirements for Business Associate Agreements (effective April 21, 2005)

- Implement safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits;
- Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate safeguards;
- Report to the covered entity any security incident of which it becomes aware; and
- Make its policies and procedures, and documentation required by the Security Rule relating to such safeguards, available to HHS for purposes of determining the CE's compliance with the regulations



# May a Covered Entity Allow a Business Associate to Merge PHI with Non-Covered Data?

- Covered entities may allow business associates to perform “*data aggregation*”
- But *data aggregation* “means, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate **with the protected health information received by the business associate in its capacity as a business associate of another covered entity**, to permit data analyses that relate to the health care operations of the respective covered entities.”

45 CFR 164.501



# That Brings Us to Some Problems for a CoC that Becomes a Business Associate

- If a CoC is the business associate of the few HIPAA-covered entities in its network, it arguably has to segregate their PHI from the data it receives from non-HIPAA-covered entities (even if it is permitted to do data aggregation among the HIPAA-covered entities).
- With respect to the data of HIPAA-covered entities, the CoC needs to determine if HMIS security levels that meet the “baselines” of the HMIS standards are sufficient.
- If not, the CoC needs to decide whether to apply different levels of security to the PHI and non-PHI.
- HIPAA’s “research” standard is far more limiting on free access by academic researchers than is the HMIS standard.
- Is the CoC performing functions “for or on behalf of” the CE?



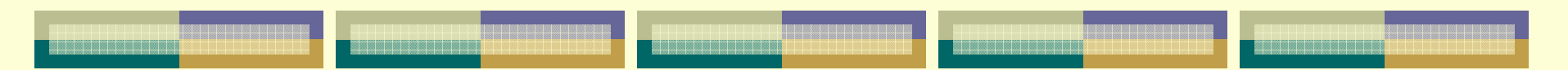
# An Alternative Approach: Use of 45 CFR 164.512

- Can the disclosure of data by a HIPAA-covered entity to a CoC be justified under one or more of the following provisions:
  - “As required by law” (164.512(a)), particularly in view of the Data and Technical Standards Final Notice;
  - “For public health activities” (164.512(b));
  - “Disclosures about victims of abuse, neglect or domestic violence” (164.512(c)); or
  - Other provisions?



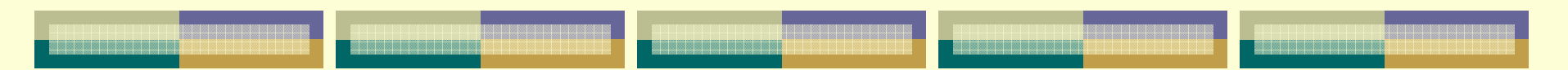
## Appendix for Discussion: HMIS Privacy Standards

If consistent with the needs and desires of the participants, we will discuss each of the optional protections, noting those that appear most valuable -- and those to avoid -- given HIPAA and related privacy experience to date.



## 4.1.3. Allowable HMIS Uses and Disclosures of Protected Personal Information (PPI)

- A CHO may use or disclose PPI from an HMIS:
  - to provide or coordinate services to an individual;
  - for functions related to payment or reimbursement for services;
  - to carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions; or
  - for creating deidentified PPI.



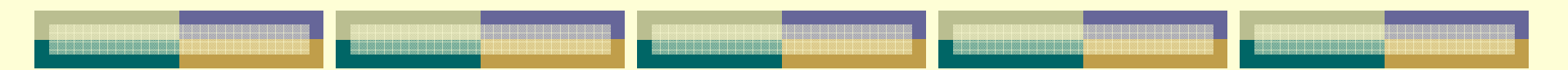
## 4.1.3. Allowable HMIS Uses and Disclosures of Protected Personal Information (PPI) (cont.)

- Uses and disclosures required by law.
- Uses and disclosures to avert a serious threat to health or safety.
- Uses and disclosures about victims of abuse, neglect or domestic violence.
- Uses and disclosures for academic research purposes.
- Disclosures for law enforcement purposes.



# HMIS Privacy Standards

- Data Collection Limitations;
- Data Quality;
- Purpose and Use Limitations;
- Openness;
- Access and Correction; and
- Accountability



## 4.2.1. Collection Limitation

### *Baseline requirement*

- A CHO may collect PPI only when appropriate to the purposes for which the information is obtained or when required by law.
- A CHO must collect PPI by lawful and fair means and, where appropriate, with the knowledge or consent of the individual.
- A CHO must post a sign at each intake desk (or comparable location) that explains generally the reasons for collecting this information.



# Collection Limitation

## *Optional Elements*

- Restricting collection of personal data, other than required HMIS data elements;
- Collecting PPI only with the express knowledge or consent of the individual (unless required by law); and
- Obtaining oral or written consent from the individual for the collection of personal information from the individual or from a third party.



## 4.2.2. Data Quality

### *Baseline Requirement*

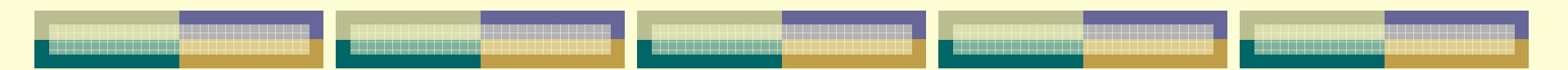
- PPI collected by a CHO must be relevant to the purpose for which it is to be used. To the extent necessary for those purposes, PPI should be accurate, complete and timely.
- A CHO must develop and implement a plan to dispose of or, in the alternative, to remove identifiers from, PPI that is not in current use seven years after the PPI was created or last changed (unless a statutory, regulatory, contractual, or other requirement mandates longer retention).



## 4.2.3. Purpose Specification and Use Limitation

### *Baseline Requirement*

- A CHO must specify in its privacy notice the purposes for which it collects PPI and must describe all uses and disclosures.
- A CHO may use or disclose PPI only if the use or disclosure is allowed by this standard and is described in its privacy notice. A CHO may infer consent for all uses and disclosures specified in the notice and for uses and disclosures determined by the CHO to be compatible with those specified in the notice.
- Except for first party access to information and any required disclosures for oversight of compliance with HMIS privacy and security standards, all uses and disclosures are permissive and not mandatory. Uses and disclosures not specified in the privacy notice can be made only with the consent of the individual or when required by law.



## 4.2.3. Purpose Specification and Use Limitation

### *Optional Elements 1*

- Seeking either oral or written consent for some or all processing when individual consent for a use, disclosure or other form of processing appropriate;
- Agreeing to additional restrictions on use or disclosure of an individual's PPI at the request of the individual if the request is reasonable. The CHO is bound by the agreement, except if inconsistent with legal requirements;
- Limiting uses and disclosures to those specified in its privacy notice and to other uses and disclosures that are necessary for those specified;



## 4.2.3. Purpose Specification and Use Limitation

### *Optional Elements 2*

- Committing that PPI may not be disclosed directly or indirectly to any government agency (including a contractor or grantee of an agency) for inclusion in any national homeless database that contains personal protected information unless required by statute;
- Committing to maintain an audit trail containing the date, purpose and recipient of some or all disclosures of PPI;
- Committing to make audit trails of disclosures available to the homeless individual; and
- Limiting disclosures of PPI to the minimum necessary to accomplish the purpose of the disclosure.



## 4.2.4. Openness

### *Baseline Requirement*

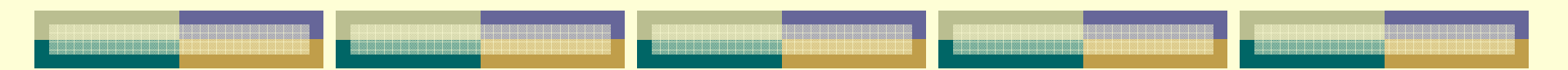
- Publish a privacy notice describing its policies and practices for the processing of PPI and must provide a copy of its privacy notice to any individual upon request.
- A CHO must post a sign stating the availability of its privacy notice to any individual who requests a copy.
- A CHO must state in its privacy notice that the policy may be amended at any time and that amendments may affect information obtained by the CHO before the date of the change. An amendment to the privacy notice regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated.



# Openness

## *Optional Elements*

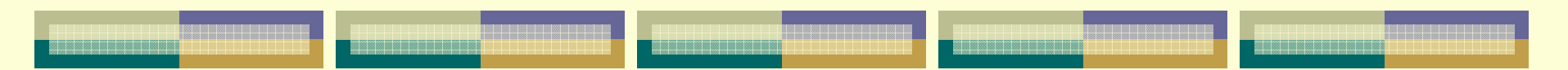
- Making a reasonable effort to offer a copy of the privacy notice to each client at or around the time of data collection or at another appropriate time;
- Giving a copy of its privacy notice to each client on or about the time of first data collection. If the first contact is over the telephone, the privacy notice may be provided at the first in-person contact (or by mail, if requested); and/or
- Adopting a policy for changing its privacy notice that includes advance notice of the change, consideration of public comments, and prospective application of changes.



## 4.2.5. Access and Correction

### *Baseline Requirement*

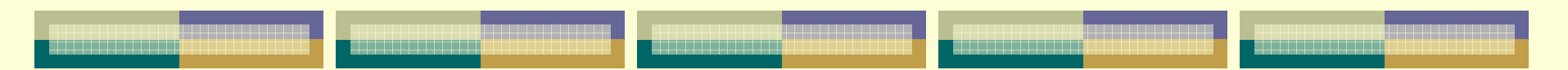
- In general, a CHO must allow an individual to inspect and to have a copy of any PPI about the individual.
- A CHO must offer to explain any information that the individual may not understand.
- A CHO must consider any request by an individual for correction of inaccurate or incomplete PPI pertaining to the individual. A CHO is not required to remove any information but may, in the alternative, mark information as inaccurate or incomplete and may supplement it with additional information.



## 4.2.5. Access and Correction

### *Optional Elements*

- A CHO SHOULD reserve the ability to rely on the following reasons for denying requests:
  - Information compiled in reasonable anticipation of litigation or comparable proceedings;
  - information about another individual (other than a health care or homeless provider);
  - information obtained under a promise of confidentiality (other than a promise from a health care or homeless provider) if disclosure would reveal the source of the information; or
  - information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual.



## 4.2.5. Access and Correction

### *Optional Elements (cont.)*

- Accepting an appeal of a denial of access or correction by adopting its own appeal procedure and describing the procedure in its privacy notice;
- Limiting the grounds for denial of access by not stating a recognized basis for denial in its privacy notice;
- Allowing an individual whose request for correction has been denied to add to the individual's information concise statement of disagreement. A CHO may agree to disclose the statement of disagreement whenever it discloses the disputed PPI to another person. These procedures must be described in the CHO's privacy notice; and/or
- Providing to an individual a written explanation of the reason for a denial of an individual's request for access or correction.



## 4.2.6. Accountability

### *Baseline Requirement*

- A CHO must establish a procedure for accepting and considering questions or complaints about its privacy and security policies and practices.
- A CHO must require each member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign (annually or otherwise) a confidentiality agreement that acknowledges receipt of a copy of the privacy notice and that pledges to comply with the privacy notice.



## 4.2.6. Accountability

### *Optional Elements*

- Requiring each member of its staff (including employees, volunteers, affiliates, contractors and associates) to undergo (annually or otherwise) formal training in privacy requirements;
- Establishing a method, such as an internal audit, for regularly reviewing compliance with its privacy policy;
- Establishing an internal or external appeal process for hearing an appeal of a privacy complaint or an appeal of a denial of access or correction rights; and/or
- Designating a chief privacy officer to supervise implementation of the CHO's privacy standards.



# Questions and Answers

For more information:  
Jon Neiditz  
(678) 427-7809  
[jneiditz@hunton.com](mailto:jneiditz@hunton.com)