pennsylvania
DEPARTMENT OF COMMUNITY
& ECONOMIC DEVELOPMENT

2017 PENNSYLVANIA HOMELESS MANAGEMENT INFORMATION SYSTEM

PRIVACY & SECURITY STANDARDS

January 8, 2017

pennsylvania DEPARTMENT OF COMMUNITY & ECONOMIC DEVELOPMENT

Privacy & Security Standards

Agenda

- Privacy vs. Security
- General Definitions
- Standards Application (Who does this apply to?)
- Privacy Responsibilities
  - 6 Separate Requirements
  - Privacy Notice and Posting
- Security Standards Responsibilities
  - PA HMIS Vendor Duties
  - CHO and System User Duties
- Conclusion

Privacy & Security Standards
Privacy vs. Security

- Privacy
  - Is the control over the extent, timing, and circumstances of sharing oneself (physically, behaviorally, or intellectually) with others.

    Privacy consists of ensuring specific measures are in place when dealing with personal information and includes directives on when it is collected, how that information is used and how that information is shared with others.

- Security
  - Is the means of ensuring that data is kept safe from corruption and that access to it is suitably controlled.

    Security is all about access to actual client data, whether that data is electronically based or paper (hard copy) based.

Privacy & Security Standards Definitions

- Covered Homeless Organization (CHO) –
  - *Any organization (employees, volunteers, and contractors) that records, uses or processes Protected Personal Information. This is what we commonly refer to within PA HMIS as an Agency and includes all associated staff.*
- Personal Protected Information (PPI) –
  - *Any information about a homeless client that (1) identifies a specific individual, (2) can be manipulated so that identification is possible, (3) can be linked with other available information to identify a specific individual*
  - *Includes name, SSN, program entry/exit, zip code of last permanent address, system/program ID, and program type*

Privacy & Security Standards
Standard Application

- Applies to all Agencies and Programs that record, use or process Protected Personal Information (PPI) within PA HMIS.
- This includes:
  - Balance of State CoC,
  - Homeless service providers,
  - PA HMIS staff, AND
  - Any employees, volunteers, affiliates, contractors and associates who have access to the PA HMIS or PA HMIS client information. This also means that any homeless service provider who does not receive HUD funding, such as faith based organization, or a city, county or state agency that is accessing the system or client data, must also adhere to the privacy and security requirements.
- Privacy and Security applies to ALL agencies and programs entering data into PA HMIS, regardless of funding source.

Privacy & Security Standards
Standard Application

Privacy Standards:

- Protect client personal information from unauthorized disclosure
- Allow for reasonable, responsible data disclosures
- Derived from principles of fair information practices

Six Components of Privacy:

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

Privacy & Security Standards

Data Collection Limitations and Data Quality

Data Collection:

- A CHO may collect PPI only when appropriate to the purpose for which the information is obtained or when required by law; PPI must be collected by fair and lawful means.
- A CHO must post a sign at each intake desk (or comparable location) that explains generally the reasons for collecting this information. An example consumer notice we be shown at the end of the privacy section.

Data Quality:

- PPI collected by a CHO must be relevant to the purpose for which it is used and should be accurate, complete, and timely

Privacy & Security Standards

Purpose and Use Limitations

- 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 disclose or use PPI only if the use or disclosure is allowed by this standard and is described in its privacy notice
- Uses and disclosures not specified in the privacy notice can be made only with the consent of the individual or when required by law

Privacy & Security Standards

Openness

- A CHO must publish a privacy notice describing its policies and practices for the processing of PPI and 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

Privacy & Security Standards

Access and Correction

In the interest of client access and full disclosure to their own PPI every CHO must:

- Allow an individual to inspect and to have a copy of any PPI about the individual, this includes access to any electronic data entered into PAHMIS or hard copy files on the premises.
- Offer to explain any information that the individual may not understand
- 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, alternatively, mark information as inaccurate or incomplete and supplement it with additional information

Privacy & Security Standards

Accountability

- 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

Privacy & Security Standards

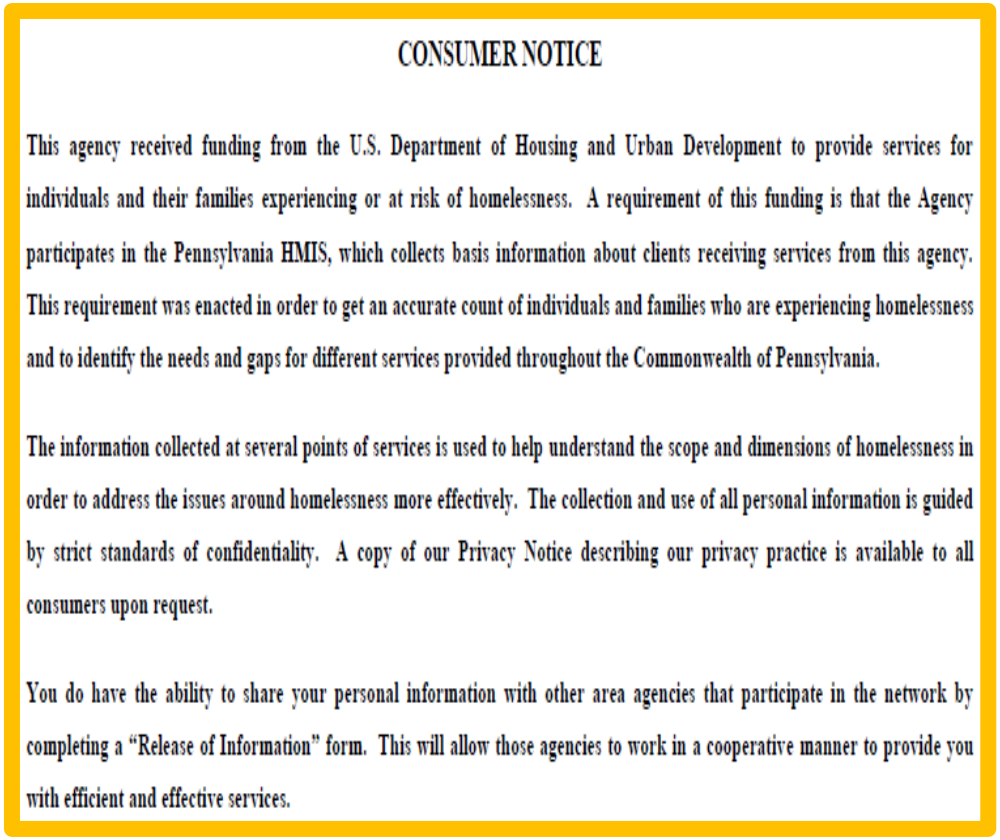
Accountability

In summary, every CHO that collects, uses and shares PPI must have a published Privacy Notice and it must be maintained and made available to the general public and meet the following:

- Must also comply with other federal, state, and local confidentiality law
- Recommended to have a history of updates recorded for each published version (version control system)
- Recommended to post on web site (if applicable)

Privacy & Security Standards

Accountability



CONSUMER NOTICE

This agency received funding from the U.S. Department of Housing and Urban Development to provide services for individuals and their families experiencing or at risk of homelessness. A requirement of this funding is that the Agency participates in the Pennsylvania HMIS, which collects basis information about clients receiving services from this agency. This requirement was enacted in order to get an accurate count of individuals and families who are experiencing homelessness and to identify the needs and gaps for different services provided throughout the Commonwealth of Pennsylvania.

The information collected at several points of services is used to help understand the scope and dimensions of homelessness in order to address the issues around homelessness more effectively. The collection and use of all personal information is guided by strict standards of confidentiality. A copy of our Privacy Notice describing our privacy practice is available to all consumers upon request.

You do have the ability to share your personal information with other area agencies that participate in the network by completing a "Release of Information" form. This will allow those agencies to work in a cooperative manner to provide you with efficient and effective services.

A Privacy posting or consumer notice or sign must be displayed at each intake desk or comparable location that explains: (at the least)

- Reason for data collection
- Availability of the CHOs Privacy Notice describing the privacy practices to all clients/ consumers that request a copy.
- Additional information that can be placed on the consumer notice is any additional data sharing disclosures or data collection rules, such as giving notice to all clients that apply for services that by accepting services they have given implied consent to having their data collected and entered into PA HMIS.

Privacy & Security Standards

Security Categories

EccoVia, Inc. (HMIS Vendor), PA HMIS/ DCED and CHOs must apply system security provisions to all the systems where personal protected information is stored, including, but not limited, a CHO's networks, desktops, laptops, cell phones, tablet and/ or portable devices, mainframes and servers.

Security has three categories:

- System Security
- Software Application Security
- Hard Copy Security

Privacy & Security Standards

Security

EccoVia, Inc, in accordance with DCED, adheres to the following standards and is in compliance in the following mandates:

- Virus Protection - must protect HMIS systems from viruses by using commercially available virus protection software
- Firewalls - must protect HMIS systems from malicious intrusion behind a secure firewall
- Disaster Recovery and Backup - must copy all HMIS data on a regular basis to another medium (e.g., tape) and store it in a secure off-site location where the required privacy and security standards would also apply
- Electronic Data Transmission - must encrypt all HMIS data that are electronically transmitted over the Internet, publicly accessible networks or phone lines to current industry standards
- Electronic Data Storage - must store all HMIS data in a binary, not text, format
- System Monitoring - must use appropriate methods to monitor security systems
- Disposal - in order to delete HMIS data, the original storage medium must be properly formatted

Privacy & Security Standards

CHO System Security

- Each CHO Workstation (computer or portable device) should have a specific username and password that allows for Windows access and should be non generic in nature. *(Example do not have each computer logon as User and No Password or User and Password of 1234.)*

- Workstation should be locked or have a time out mechanism after a period of inactivity (i.e. 10 -20 minutes) that places the computer into a password enabled screen saver state whereas the username and password must be re-entered in the computer to allow access again.

- Many workstations have windows application (i.e. word or pdf documents and email) that could potentially contain PPI and need to be secured accordingly.
  - *A Case Worker could be sending an email about a client to an outside Agency resource or medical clinic and this information needs to be guarded as well as any information that even contains the clients name falls under into this PPI category.*

Privacy & Security Standards

CHO Software Application Security

- Each CHO User must have an individual username and password that is used to Log On and Use PA HMIS.
- Written information specifically pertaining to user access (i.e. username and password) may not be stored or displayed in any publicly accessible location.
- PA HMIS Users must not provide their user access to any other member of their CHO and shared user access is strictly prohibited within the Participation Agreement and System User Agreement. Under no circumstances should any PA HMIS user give you're their personal username and password to any other CHO users, this includes their supervisor or management team.

Privacy & Security Standards

CHO Hard Copy Security

- A CHO must secure any paper or other hard copy containing personal protected information that is either generated by or for HMIS, including, but not limited to reports, data entry forms and signed consent forms.
- A CHO must supervise at all times any paper or other hard copy generated by or for HMIS that contains PPI when the hard copy is in a public area.
- When CHO staff are not present, the information must be secured in areas that are not publicly accessible.
- ***We highly recommend keeping your files in a securely locked room or closet that can closed up when all staff have left for the night or weekend.***

Privacy & Security Standards

Additional CHO Security

The following are additional security measures that should be put in place to reduce the physical access to confidential client data:

- Escort all visitors and clients to ensure that they do not access staff areas, record storage areas, or other areas potentially containing client information, and the CHO will request persons not recognized as staff, visitors and Clients to identify themselves.
- Implement security measures to prevent unauthorized use of photo copiers, printers and fax machines by visitors and other unauthorized persons.
- Create an atmosphere where the CHO staff feels comfortable and obligated to report security breaches and misuse of the PA HMIS system. All CHOs should encourage clients to report any breaches of confidentiality that they observe at the CHO or by CHO staff members.

Privacy & Security Standards

Conclusion

- Privacy is in everyone's hands and it is all of our responsibilities to ensure client's Personal Protected Information (PPI) remains confidential, relevant and only in front of authorized personnel,
- Please ensure all CHOs review their privacy notices and policies with staff on a regular basis,
- The Security Standards presented for CHOs are not difficult to implement and can significantly lower the chance of unauthorized access occurring.

For specific program information:
http://www.pennsylvaniacoc.org/pahmis/

Pennsylvania Homeless Management Information System

HUD Issued Guidance
Tools and Technical Assistance Resources
FAQs and Resources

Proposed Rule for HMIS Requirements

- https://www.hudexchange.info/resource/1967/hearth-proposed-rule-for-hmis-requirements/

PA Homelessness Contacts

- David Weathington, Economic Development Analyst
  - dweathingt@pa.gov or (717) 720 - 7304
- PA HMIS Help Desk
  - RA-pahmis@pa.gov or (717) 214 - 5326