Arkansas All-Payer Claims Database Data Protection

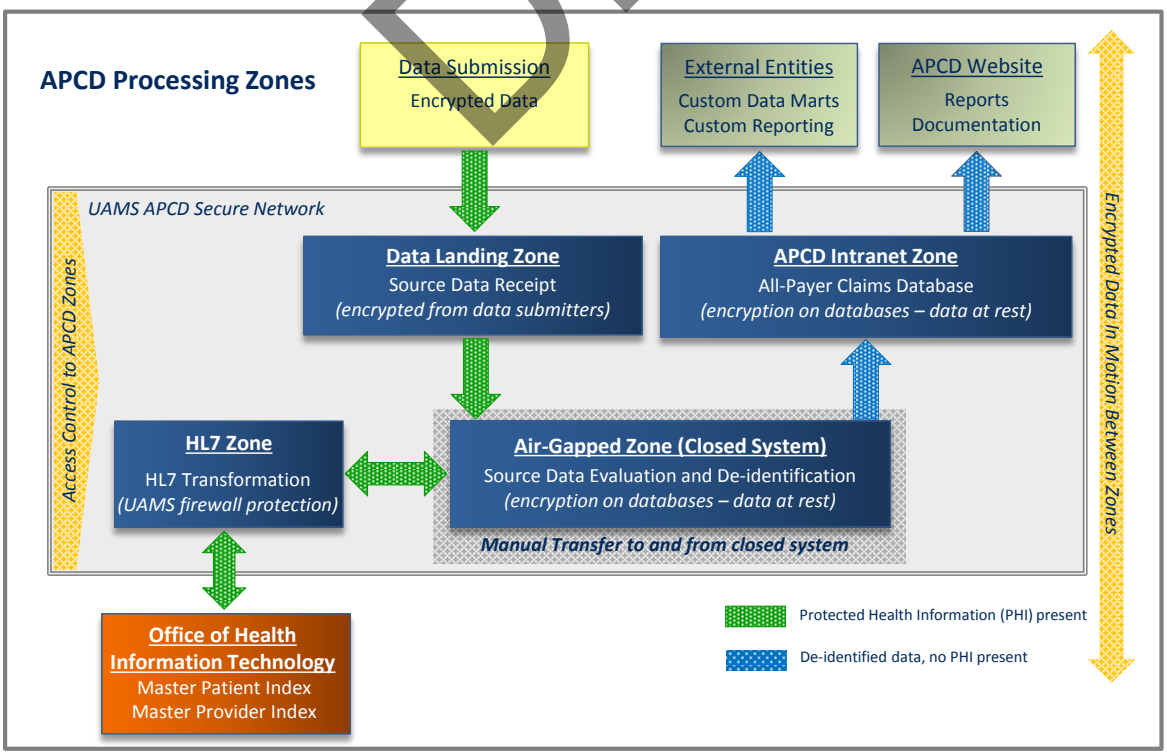
The security of protected health information (PHI) is a critical component of the University of Arkansas for Medical Sciences' (UAMS) Arkansas Center for Health Improvement (ACHI) All-Payer Claims Database (APCD) data security strategy. The Health Insurance Portability and Accountability Act (HIPAA) generally defines PHI as individually identifiable health information that is transmitted or maintained in any form or medium by an entity covered by HIPAA or its business associate. HIPAA requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of PHI.

As part of the APCD project, ACHI will be collecting, warehousing, and analyzing PHI. All data for the APCD, including PHI, are encrypted and protected, but personally identifiable information will never appear in any public APCD data output or report. All data within the APCD are protected while **'in motion'**—as they are transferred from platform to platform for processing. They are also protected while they are **'at rest'**—when stored within any APCD server or database to prevent unauthorized access to or use of submitted data. ACHI APCD data protection solutions are described in the table below.

Data Protection Solution	Description
Data submission and/or data receipt authorization	Each data submitter receives authorization to submit data after **data use agreements** are in place. Entities requesting data receive authorization through the data release process.
SFTP and encryption keys	Unique **secure file transfer protocols (SFTP)** and **encryption keys** are established for each authorized entity to protect data in motion.
UAMS information technology security protocols	**UAMS network security,** including internal and external **firewalls**, and **user authorization** at different levels are used to protect data in motion and at rest.
APCD Air-Gapped Zone	The APCD Air-Gapped Zone (AGZ) is a **closed system where PHI is stored and data is de-identified**. This closed system has no physical connection with the UAMS network or Internet. Only **authorized personnel** can access the AGZ.
Server and database encryption	All APCD **servers are encrypted**, protecting them against unauthorized access. **Encrypted media** are used to protect data when manual data transfer is required. APCD **databases are encrypted** to protect data at rest.
Data access authorization	Each data touch point is **restricted to authorized personnel** only, protecting data from unauthorized access throughout its journey through the APCD process.

Figure 1 illustrates the path data follows as it is received and processed through the APCD processing zones and the data protections used throughout processing.

Figure 1: Data Touch Points and Protection Protocols



What does encrypted data look like?

Encryption is the primary tool used within the APCD to protect data. It translates information into unreadable letter, number, symbol, and punctuation combinations and is very effective in protecting data content from being accessed and utilized by unauthorized individuals, such as malicious hackers. Encryption is controlled by encryption keys that, when applied, translate the encrypted information into useable data. Encryption keys are available only to limited, authorized personnel.

Unencrypted data example:

```
Joe Smith,123 Main Street, El Paso, AR, 72045, White, 01-01-1980, 123-45-6789
```

Without the encryption key, data will look like this:

…‹·ÿö¦ô¤g–M?ƒèZ¤9,`•ký^GÊU_xOÚž§Ü L øw‹‰Ë•y*¶…z¹x*±+?;n•
B,Ó“8¸’¼ìk3ãïï½n•~Êa…ÿ¼-y½ª„:!u`Ø³ë)-œlâÛÑª÷±¢@d¶3XËíÚ

What is de-identification?

De-identification is the process of removing or transforming personally identifiable information (PII) to prevent a person's identity from being connected with personal health information. Several de-identification strategies are utilized including replacing PII with unique APCD identifiers, replacing date of birth with an age value, and, for those ZIP code ranges having fewer than 20,000 residents, ZIP codes are reduced to the first 3 digits.

In the example below, the Input Record contains PII including name, address, city, state, ZIP code, date of birth, and Social Security Number.

Input Record:

Name	Address	City	State	ZIP	County	Date of Birth	Social Security Number
Joe Smith	123 Main Street	El Paso	AR	72045	White	01-01-1980	123-45-6789

De-identification processing will replace the name, address, city, ZIP code, date of birth, and Social Security Number with an APCD identifier value from the Input Record above. Additionally, the date of birth is replaced with an age value, and the input ZIP code is reduced to its first three digits. Independently, State and County values are not treated as PII and remain unchanged.

Output Record:

APCD Identifier	State	ZIP 3	County	Age Value
AP1P0000QX03482	AR	720	White	34

What data release protection protocols are in place?

PHI will never appear in any public APCD data output or report. All requests for APCD data must meet APCD data request requirements. Entities requesting data must detail the purpose of each project, the methodology, the qualifications of the requesting entity, and, by executing a data use agreement, comply with the requirements of the HIPAA. The APCD Data Release Committee reviews each request, determines whether the release of data is consistent with the mission and objectives of the APCD and contributes to efforts improving health care for Arkansans.

ARKANSAS APCD All-Payer Claims Database