HUMAN RESOURCES & BENEFITS INFORMATION

HIPPA FLOW CHART

Questions and Answers

1. Does the plan exist for purposes of providing or paying for the cost of medical care?

A health plan could be an individual or a group health plan for purposes of HIPAA. A health plan includes (but is not limited to) employer sponsored benefit plans like those covered under ERISA, health insurers, HMOs, group health plans, and many public benefit programs (Medicare and Medicaid).

You would respond 'Yes' if your city has any of the following types of plans:

- Medical
- Dental
- Vision
- Prescription drug
- Behavioral Health
- Wellness plan that provides health benefits
- EAP that provides health benefits
- High Deductible Plan
- Health Reimbursement Arrangements (HRAs) – including a Post Employment Health Care Savings Plan
- Flex Plan (medical reimbursement portion)
- Long-term care

Examples of plans in which the city would respond 'No' include:

- Long term and short term disability (income replacement)
- Workers Compensation
- Life Insurance
- Flex plans (portions covering child care expenses)
- Other non-health plans

2. Does the plan provide health benefits through a contract for insurance with a state licensed insurance carrier or HMO?

A contract for insurance is not a contract for administrative services – it essentially means that the city is covered under a fully insured plan. See § 164.520(a)(2) and related sections of the Final Privacy Rule for more detail.

If the plan meets the criteria above (benefits provided through a contract for insurance with a state licensed carrier or HMO), the city would respond 'Yes'. Unless the plan meets all the criteria, you would respond 'No'. For example:

- If the plan participates in a pool through a contract / joint powers agreement with an entity which is not a health insurance issuer or an HMO, you would answer 'No' (e.g. coverage through the Service Cooperatives).
- If the contract between the plan and the insurance issuer or HMO is for administrative services only (i.e. third party administrative services), you would answer 'No'.
- If the plan pays any or all of the insurance claims of its members (essentially the plan is self-insured), you would respond 'No'.

3. Are there more than 50 participants in the health plan?

HIPAA provides a limited exemption for those plans that (a) have less than 50 participants, (b) are self-insured, **and** (c) self-administer their own plan. All three requirements must be met. Health plans that have more than 50 participants and/or contract with a third party to administer the plan do not qualify for the exemption.

A "plan participant" is an employee who is eligible for and actually participating in the health plan. However, cities that have close to 50 participants will need to be aware of the HIPAA requirements in the event that they go over 50 employees in the future.

4. Is the health plan self-administered?

Again, HIPAA provides an exemption for those plans that have less than 50 participants **and** self-administer their own plan. Any other arrangements for services, such as a contract with a third party to administer claims processing, enrollment, billing, etc. (or plans with more than 50 eligible participants), do not qualify for the exemption. See §160.103 Definitions of the Final Privacy Rule for more information.

5. Does the City receive more than enrollment / disenrollment and summary health information?

Enrollment / disenrollment information is information regarding a person's eligibility for and election to participate under a HIPAA covered health plan. Summary Health Information is information that summarizes claims history, claims expenses, and types of claims experience by individuals under a health plan provided it has been de-identified with the exception that it may include five digit zip codes.

- Names
- Geographic units (e.g. Apt or house number, street address, city)

- Dates related to an individual, including birth date, admission date, discharge date, date of death
- Ages
- Telephone numbers and fax numbers
- E-mail addresses
- Social security numbers
- Medical record numbers, health plan beneficiary numbers, account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs) and Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code

All of these identifiers would have to be removed for you to answer 'No. If you receive claims data with **any** of the identifiers listed above, you would respond 'Yes'.

Note: If you receive information with these kinds of identifiers, then the city may want to evaluate whether or not they really need this information for purposes of sponsoring the health plan. If they don't need this information, then the city may want to discontinue receiving it.

6. The plan is a covered entity under HIPAA but has minimal responsibility for complying with the Administrative Simplification regulations.

Based on the information provided, this plan has **minimal responsibilities** under HIPAA. The plan must:

- Not require any member to waive their HIPAA rights as a condition for enrolling in a health plan, eligibility for benefits, treatment or payment of health care expenses.
- Not discriminate on the basis of any health condition.
- Amend plan documents if you want access to protected health information from the group health plan (Note: This may increase your responsibilities under HIPAA).
- Obtain authorization from the individual in cases where they may seek your assistance with a health claim or appeal involving the health insurer.

Because the plan does receive protected health information (albeit limited PHI) such as enrollment and eligibility information, the plan must also get a Business Associate Agreement with their broker and anyone else doing anything on their behalf that receives PHI. Under HIPAA, the plan is not required to get a Business Associate Agreement with the carrier/HMO [fully insured plans only] or the plan's sponsor/employer.

7. The plan is a covered entity under HIPAA and is required to comply with all of the Administrative Simplification regulations.

Based on the information provided, this plan must comply with **all** of HIPAA's Administrative Simplification requirements that relate to health plans, including:

- Modifying plan documents to permit information sharing between the group health plan and the plan sponsor, and institute procedures for complying with those amendments.
- Designating a privacy official. This individual is responsible for ensuring the procedures are followed and has the authority to make determinations about what and how information can be released. This could be the city's data practice official.
- Designating who may access Protected Health Information.
- Establishing firewalls to limit or restrict the flow of information between the group health plan and the employer as the plan sponsor.
- Creating and implementing policies and procedures and maintain documentation.
- Complying with the privacy rules regarding use and disclosure of protected health information – obtain authorization or consent as required.
- Certifying to your carrier/HMO that you are HIPAA compliant.
- Issuing a Notice of Privacy Practices to employees.
- Identifying Business Associates (such as third party administrators and/or the city's agent/broker) and amend contracts with each to ensure that these entities take steps to comply with HIPAA.
- Obtaining authorization or consent in order to receive or disclose protected health information.
- Training employees who use or disclose protected health information on the plan's privacy policies and procedures.
- Developing a grievance procedure for individuals challenging or disputing the use or disclosure of health information.
- Tracking certain types of member information requests for six years.
- Allowing members to amend their medical records.
- Allowing members to restrict access to certain medical information.

Please be aware that some of these functions may be delegated to the city's third party administrator through the business associate agreement, which should outline what responsibilities the city has as the covered entity in regards to HIPAA compliance and what responsibilities the TPA has as the business associate.

Even if you delegate responsibilities to your business associate(s), the city is not entirely off the hook – you still have an obligation to make sure that the business associate is complying with HIPAA. For instance, you should review the business associate agreement annually and/or request reports or documentation showing compliance activities on the part of the business associate (these reports could be requested annually, semi-annually or quarterly).

8. Does the covered entity store, maintain or transmit PHI electronically?

In order to respond to this question, covered entities **must** conduct a risk assessment/analysis and document their determinations regarding whether the security measures apply to them or not. There is no exception for small health plans (other than the delayed effective date and the exception for small self-administered plans – see FAQ #7). Therefore, all group health plans, whether self-administered, self-insured and administered by a third party administrator, or fully insured, must evaluate the extent to which they must comply (if at all) to the security standards. The security standards build upon the HIPAA privacy rules and are intended to protect the privacy and confidentiality of electronic protected health information (E-PHI) from improper access and interception. They are designed to ensure that electronic health information is accurate and accessible only to certain people.

The security rules apply to protected health information that is electronically maintained or used in an electronic transmission, regardless of format (for a definition of protected health information, see #4 under the FAQ). E-PHI is PHI in electronic media such as through the Internet, leased lines, dial-up lines and private networks. Telephone voice response and faxback systems are covered under the security standards, but not paper-to-paper faxes, video conferencing or messages left on voicemail. There is no distinction between internal or external communications, so even internal transactions must meet the requirements.

Examples of a "Yes" response may include:

- Conducting enrollment, disenrollment and/or billing online.
- E-mail communications with employees and/or the health insurance carrier or third party administrator that contains PHI.
- The city self-administers its health flexible spending account under the cafeteria plan and stores all claims information in a database on the computer system.

Examples of a "NO" response might include:

- The city faxes an explanation of benefits that they received from an employee on a claim issue to the health insurance carrier [Caution: Still HIPAA privacy concerns].
- The city receives quarterly claims information that is provided in aggregate form with no individually identifiable information.
- The city does not store any PHI on the computer (all information is kept in hard copy in locked file cabinets) – note: one e-mail to the health insurance carrier or TPA that contains PHI will likely subject the city to the security standards.

9. The plan is subject to the HIPAA security standards.

The good news is that the security rules allow covered entities some flexibility to determine which of the security measures are appropriate for their circumstances. The security standards are designed to be general and flexible enough to be used in varying degrees according to the size of the covered entity, sophistication and financial capability.

The security requirements can be broken down into five categories:

- Administrative safeguards
- Physical safeguards
- Technical safeguards
- Organizational requirements
- Policies, procedures and documentation requirements

More information about each of these requirements can be found by going to the HIPAA Security Overview information sheet. The League is also working to develop templates of policies and procedures relating to the security standards. Member cities may contact the League's HR & Benefits Department at 651-215-4095 or 800-925-1122 to request a copy of this additional tool.

10. The plan is NOT subject to the HIPAA security standards.

Even if you determine that your city is not subject to the HIPAA security standards, it is important that you first conduct the risk analysis and document your determination regarding the city's need to comply (or not) with the security standards.

It is also important to realize that a simple e-mail containing PHI may subject the city to the security standards. Cities currently not subject to the security standards may need to monitor and evaluate this matter on an ongoing basis to ensure that the city is ready to comply at any given point and time during the year if necessary.