Date: May 3, 2018
To: Joint Labor-Management Benefits Committee
From: Staff
Subject: Benefits Provider Information Exchange

RECOMMENDATION
That the JLMBC receive and file staff report including the joint memorandum from Keenan & Associates and Segal Consulting regarding the exchange of patient information with the LAwell Civilian Benefits Program’s health plan carriers.

DISCUSSION
At its February 8, 2018 meeting, the JLMBC requested that staff research the feasibility of the LAwell Civilian Benefits Program’s vision and dental service providers, EyeMed and Delta Dental, sharing patient information with health plan carriers, Kaiser and Anthem with the goal of improving the efficiency and effectiveness of patient care. Staff and benefits consultants, Keenan & Associates (Keenan) and Segal Consulting (Segal), met with EyeMed, Delta Dental, Kaiser, and Anthem to discuss available options and potential legal conditions governing the exchange of member data for fully insured plans. Based on this meeting and further research and discussions, Keenan and Segal have prepared the attached joint memorandum with their findings on the exchange of patient information with the health plan carriers and an evaluation of the capabilities and limitations. Keenan and Segal will jointly present this information (Attachment A).

Submitted by: ____________________________
Paul Makowski

Reviewed by: ____________________________
Jenny M. Yau

Approved by: ____________________________
Steven Montagna
MEMORANDUM

To: City of Los Angeles JLMBC

From: Laurie Lofranco, Keenan and Associates, Robert Mitchell and Stephen Murphy, Segal Consulting

Date: March 29, 2018

Re: Benefits Provider Information Exchange

At the February 8, 2018 meeting, the JLMBC requested that staff research the feasibility of the LAwell Civilian Benefits Program’s vision and dental coverage insurers sharing patient information electronically with Anthem and Kaiser, to alert them to potential chronic conditions identified during a member’s vision or dental exam. This memo will address the following.

- HIPAA Privacy
- Patient Authorization
- Data Exchange Prevalence and Uses

HIPAA Privacy
The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), requires “Covered Entities” and Business Associates to comply with requirements to protect the privacy and security of health information. Covered entities are defined under HIPAA as (1) health care providers, (2) health plans, and (3) health care clearinghouses.

<table>
<thead>
<tr>
<th>Health Care Provider</th>
<th>Health Plan</th>
<th>Health Care Clearinghouses</th>
</tr>
</thead>
</table>
| A person or business who, in the normal course of business, furnishes, bills, or is paid for rendering health care and transmits (sends directly or indirectly) health information electronically in connection with a HIPAA Electronic Data Interchange (EDI) transaction. | This includes:  
- Health insurance companies providing medical, dental and vision plans  
- HMOs  
- Company health plans  
Government programs that pay for health care, such as Medicare, Medicaid, and | This is a business that translates health care data from paper (non-standard format/content) to electronic (standard format/content) or vice versa. |
The Anthem, Kaiser, Delta Dental, and EyeMed plans, as well as their contracted health care providers, are covered entities under HIPAA. This means that each insurer and contracted provider is obligated to comply with HIPAA Privacy, Security and Breach regulations.

HIPAA permits a covered entity to share a patient’s protected health information (PHI) with another covered entity for the purposes of Treatment, Payment and health care Operations (TPO). For example, an optometrist could alert the patient’s Primary Care Physician (PCP) of potential signs of diabetes or other health conditions identified during the member’s vision exam.

While covered entities may exchange PHI, HIPAA restricts electronic exchanges to the minimum data necessary to accomplish the required task. As a result, an electronic file exchanged between two insurers may be TPO, but if the file includes all participants, this could violate HIPAA’s minimum necessary requirement.

Patient Authorization

Covered entities are required to obtain a patient’s advance written permission to use/disclose PHI (except for limited situations allowed under HIPAA as explained in the paragraph above) by using a HIPAA authorization form. The form is a customized document that permits use/disclosure of health information for specific reasons and for a specified time. It is typically updated annually or completed prior to an initial visit, and may include the Primary Care Physician’s contact information. Sample HIPAA authorization and termination forms are included for your reference.

Data Exchange Prevalence and Uses

A. Outbound Data Capabilities - Delta Dental and EyeMed

Delta Dental – Delta Dental originally advised that they exchange electronic PHI files for their self-funded plans, but they do not exchange this information for their fully insured plans. Because the distinction between self-funded and fully insured plans was not clear, Delta Dental was asked to provide clarification. After reconsideration, they agree that both California law and federal HIPAA do allow Delta Dental to share information with other covered entities, with a signed HIPAA patient authorization. Because Delta Dental does not receive diagnosis codes from dentists, they are limited to sharing procedural codes, like periodontal treatments, which could be an indicator of chronic disease like diabetes.

EyeMed - EyeMed indicated electronic PHI exchanges between insurers are permissible, without member consent, under HIPAA’s TPO provisions as long as the requirements outlined below are met.

- Medical insurer specifies in writing:
  - It insures City’s medical plan;
  - It will use the data to conduct population-based activities relating to case management or care coordination;
The data elements insurer is requesting;
That these data elements are the minimum PHI necessary;

EyeMed currently transfers files on behalf of two self-funded clients and six fully insured clients. Five of these entities are private sector clients while the other three are school districts. One of the insured clients involves Anthem. However, because Mercer’s eligibility file does not currently identify which medical plan employees are enrolled in, EyeMed would not know which vendor (i.e., Anthem or Kaiser Permanente) should receive the electronic PHI data.

B. Inbound Data Capabilities – Kaiser and Anthem

Kaiser - Kaiser indicated that because it relies on its proprietary integrated electronic medical record and evidence based algorithms to identify and close potential gaps in care, they would not integrate Delta Dental or EyeMed data into their electronic medical record data.

Anthem – Similar to Kaiser, Anthem confirmed it is not able to integrate EyeMed data for its HMO plans. However, Anthem has indicated it can integrate EyeMed’s information with its PPO medical data only to target and stratify members eligible for disease management programs (i.e., Asthma, Chronic Obstructive Pulmonary Disease, Congestive Heart Failure, Coronary Heart Disease, and Diabetes). Members identified as medium to high risk due to missed medical appointments or lack of prescription refills would receive outbound engagement calls. Limitations associated with Anthem’s systems for its PPO members include:

- Inability to identify participants with High Blood Pressure; and
- Inability to identify new diagnoses not in the patient’s current medical records.

Conclusions

Currently, EyeMed providers are required to both document high risk conditions as well as refer the patient accordingly to his/her medical provider. EyeMed providers are not required to conduct additional outreach to ensure patients follow-up with their physician. Delta Dental has confirmed that all dentists are trained to inform patients of potential medical issues as part of their role as a healthcare provider, but Delta Dental does not require their network dentists to report any such findings.

EyeMed has expressed a willingness to exchange electronic patient data with the City’s health plans, as long as the transfers satisfy HIPAA and HITECH requirements including the minimum data standard. Unfortunately, the Kaiser and Anthem HMOs are not capable of receiving electronic data from the City’s dental and vision providers. As a result, the potential value of electronic data exchanges would be limited to PPO medical plan participants. Given these data limitations, there is no ready option available at present to provide for electronic data exchange between the City’s dental/vision and health plan providers.

Keenan and Segal Consulting have received commitments from Delta Dental and EyeMed to identify and implement alternate solutions that encourage patients to voluntarily seek medical treatment when a chronic condition is indicated.
Please keep in mind that this commentary is intended to provide our views as employee benefits professionals and is NOT intended to provide legal, medical, or tax advice. On issues involving laws/regulations, the City should refer to its legal counsel for authoritative advice.
Authorization Form for Release of Protected Health Information (PHI)

I. __________________________________________, hereby authorize the use or disclosure of the health information as described in this authorization.

1. Specific person/organization or health care provider authorized to provide the information:

2. Specific person/organization or health care provider authorized to receive and use the information (insert your PCP’s name, address, phone):

3. Specific description of the information to be used or disclosed (Include names of individuals to whom the information pertains such as a minor child, description of information and dates, as appropriate):

4. Purpose of the request (Check one): □ At the request of the individual signing this form.
   □ Other: ________________________________________________________________________

5. Right to Revoke: I understand that this authorization is voluntary and that I have the right to revoke this authorization at any time by notifying the Provider identified in Step 1 above (in writing). I understand that such a revocation is only effective after it is received and logged by the Provider identified in Step 1 above. I understand that any use or disclosure made prior to the revocation of this authorization will not be affected by a revocation.

6. I understand that after this information is disclosed, Federal law might not protect it and the recipient might disclose it again.

7. I understand that I am entitled to receive a copy of this authorization and the information described on this form if I ask for it.

8. I understand that this authorization will expire as indicated here: □ One year from the date of this authorization.
   □ On the following date: _________________. 20__.

9. The Provider will not condition treatment, payment, enrollment or eligibility for benefits on receipt of an authorization.

10. If this authorization is for marketing purposes, this Provider is not receiving financial remuneration (payment) from the third party whose service or item is being marketed. If the authorization is for the sale of Protected Health Information, the disclosure will not result in remuneration (payment) to the Provider.

______________________________________________ ______________________
Signature of Individual Date

or

______________________________________________ ______________________
Signature of Personal Representative Date

If a Personal Representative executes this form, that Representative warrants that he or she has authority to sign the authorization form on the basis of: □ a signed Personal Representative Form; or □ Other
Form to Revoke/Terminate a Prior Authorization

I, ____________________________, hereby revoke/terminate an authorization that I made on ________________, 20___ regarding the use or disclosure of my health information.

1. Specific person/organization/or class of persons who was authorized to provide the information:

________________________________________________________

2. Specific person/organization/or class of persons who was authorized to receive and use the information:

________________________________________________________

3. Specific description of the information that was allowed to be used or disclosed.

(Include dates as appropriate):

________________________________________________________

4. I understand that the revocation/termination is only effective after it is received and logged by the Provider identified in the original Authorization I signed. I understand that any use or disclosure made prior to the date of this revocation/termination will not be affected by this revocation/termination request.

______________________________  _______________________
Signature of Individual          Date

or

______________________________  _______________________
Signature of Personal Representative Date

If a Personal Representative executes this form, that Representative warrants that he or she has authority to sign the authorization form on the basis of:

☐ A signed Personal Representative Form;

☐ Other: ________________________________