Is a Business Associate Agreement (BAA) Required? BAA Decision Checklist

Question 1: Is the vendor providing services to or on behalf of the Department using patient or member protected health information (PHI), which includes verbal, written or electronic healthcare and/or billing information?

PHI means health information that is created or received by a healthcare provider, health plan (including MaineCare) or healthcare clearinghouse (translates claims) that relates to the physical or mental health of an individual, the provision of services to the individual or payment for services, that can reasonably be used to identify an individual.

PHI is considered de- identified when the following elements are removed**:**

1. Names;
2. Street address, city, county, precinct, zip code
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Phone numbers;
5. Fax numbers;
6. E-mail addresses;
7. Social Security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data)

If even one of the above 18 identifiers will be included in the PHI to be used, disclosed, transmitted or maintained by the vendor on behalf of DHHS, then the vendor is using identifiable PHI that requires HIPAA protection. Continue to Question 2. If none of the 18 identifiers are to be shared with the vendor, STOP. No BAA is required.

Question 2: Is the vendor a provider of treatment or healthcare services? If yes, no BAA is required unless additional administrative services like practice supervision, medical directorship supervision or administrative activities, education and training services, etc. will be provide. If operational or administrative services are to be provided in addition to treatment services, then continue to Question 3.

Question 3: Does the vendor perform any of the following services on behalf of the Department?

1. accounting
2. collections
3. claims processing or administration
4. data analysis, processing or administration
5. billing
6. benefit management
7. practice management
8. medical director (administrative role)
9. legal
10. actuarial
11. consulting on operational or business functions including audit and health information technology
12. data aggregation as defined by HIPAA
13. software hosting
14. management of data or clinical services
15. utilization review
16. quality assurance
17. patient safety activities
18. accreditation bodies
19. HealthInfoNet or other regional IT exchange
20. E-prescribing gateways
21. other entity that provides data transmission services requiring routine access to PHI
22. personal health record service provider,
23. financial services
24. transcription services
25. Medicaid transportation broker
26. Private vendors that provide eligibility or pre-authorization services

If the vendor is not providing these or similar types of services, end. No BAA is required. If yes, continue, BAA required. If uncertain about whether the vendor services require a BAA, check with your supervisor or the Director of Healthcare Privacy.

<u>Health plan/Government Plan Exceptions</u>:

No BAA necessarily required for agreements between government entities. A Memorandum of Understanding between government entities that contains the appropriate safeguards may suffice. Please speak with your Privacy Officer, supervisor or the Director of Healthcare Privacy.

No BAA required where provider sends in a claim to MaineCare, and MaineCare processes such claim for provider services. (Provider and health plan do not become business associates of each other.)