NEW YORK STATE | Department of Health | Office of Health Insurance Programs

OHIP DOS Privacy Issue Notification Form

What to report: All instances of unauthorized access, use or disclosure of Medicaid Confidential Data.

When to report: As soon as possible.

How to report: Complete this issue notification form and send it to the DOS Security and Privacy Bureau's mailbox: doh.sm.Medicaid.Data.Exchange@health.ny.gov

NEW YORK STATE | Department of Health | Office of Health Insurance Programs

Security and Privacy Issue Notification Form

Instructions: Complete the form below and send to the DOS Security and Privacy Bureau's mailbox at: doh.sm.Medicaid.Data.Exchange@health.ny.gov

Please do not put Protected Health Information (PHI) into this form. For questions on how to fill out the form below contact doh.sm.Medicaid.Data.Exchange@health.ny.gov

1. Contact Information for this Incident		
Name:	Title:	Program Office:
Email address:	Work Phone:	Mobile Phone:
Choose the Role/Program Type the organization performs for the Department of Health: Choose an item.		
2. Issue Description		
Provide a brief description of the issue:		
3. Issue Details		
Date and time the issue was discovered:		
List the type of data elements involved (DOB, SSN, Name, Account #, CIN, etc.):		
Number of individual member records affected by the issue:		

4. Issue Details: The HIPAA Breach Notification Rule presumes the event to be a breach unless the organization demonstrates that there is low probability the PHI has been viewed by unauthorized personnel.

To determine the probability that the PHI has been viewed by unauthorized personnel, please answer the following questions:

1. **Was protected health information involved?** Protected Health Information (PHI) is any information about health status, provision of health care, or payment for health care that is created or collected by a covered entity (hospital, payment processing center, etc.) that can be linked to an individual.

   ☐ Yes, PHI was involved. Continue to question 2

   ☐ No, PHI was not involved. No Breach reporting required under HIPAA

2. **Was the PHI unsecured**? Unsecured means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services (HHS) in guidance, such as encryption or destruction of identifiers. The guidance can be found on the HHS website at: **www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html**
   ☐ Yes, the PHI was unsecured. Continue to question 3
   ☐ No, the PHI was secured. No breach reporting required under HIPAA:
   Describe the PHI (for example, was it verbal, paper, or electronic) and how it was secured? Was it encrypted in compliance with HHS, password protected, other?

   _____

   _____

3. **Was there an acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule**? Providers should keep in mind that a violation of the "minimum necessary" standard is not permitted by the Privacy Rule. Providers should also keep in mind that a use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures may not be a violation of the Privacy Rule.

   ☐ Yes, there was an acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule. Continue to Question 4.

   ☐ No, there was no violation of the Privacy Rule. No breach reporting required under HIPAA.

   Describe who acquired, accessed, used and/or disclosed the PHI, whether the person was authorized or unauthorized, and how the PHI was acquired, accessed, used, or disclosed:

_____

_____

4. **Does an exception apply**? Check any box below that applies:

☐ **Exception A**. A breach does not include an unintentional acquisition, access, or use of PHI by a workforce member, or person acting under the authority of a covered entity or business associate, if it:

(i) Was made in good faith; and
(ii) Was within the course and scope of authority; and
(iii) Does not result in further use or disclosure in a manner not permitted by the Privacy Rule. (Workforce includes employees, volunteers, trainees, and other persons whose work is under the direct control of the entity, whether they are paid by the covered entity. A person is acting under the authority of a covered entity or business associate if he or she is acting on its behalf at the time of the inadvertent acquisition, access, use or disclosure.)

☐ **Exception B**. A breach does not include an inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received is not further used or disclosed in a manner not permitted by the Privacy Rule.

☐ **Exception C**. A breach does not include disclosure of PHI where the provider or business associate has a good faith belief that the unauthorized person who received it would not reasonable have been able to retain the information. (For example, PHI sent in the mail and returned by the post office, unopened, could not reasonably have been read or otherwise retained by an unauthorized person. Or, if a nurse mistakenly hands a patient the discharge papers belonging to another patient, but quickly realizes her mistake and takes back the paperwork, the nurse can reasonably conclude that the patient could not have read or otherwise retained the information. These incidents would not constitute reportable breaches.)

☐ Yes, an exception applies. No breach reporting required under HIPAA

☐ No, an exception does not apply. Continue to section 5 Risk Assessment.

5. **Risk Assessment.** An acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule is presumed to be a beach and must be reported unless the covered entity demonstrates that there is a low probability that the PHI has been compromised based on the risk assessment of at least the factors listed below. (Note: You MUST document your consideration of ALL factors listed below.

Factor A. Consider the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification if the PHI is de-identified. Consider whether the more sensitive financial information was involved, such as credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud. For clinical information, this may involve consideration of not only the nature of the services (mental health, Sexually Transmitted Disease (STD), cosmetic surgery) but also the amount of detailed clinical information involved (diagnosis, medication, medical history, test results). Consider whether the PHI could be used in a manner adverse to the patient or to further the unauthorized recipient's own interest.

Describe the PHI involved, including identifiers:

_____

_____

Explain whether PHI could be used in a manner adverse to the patient or to further the unauthorized person's interest:

_____

_____

Factor B. Consider the unauthorized person who used or received the PHI. This factor must be considered if the PHI was impermissibly used within the facility as well as when the PHI is disclosed outside the facility. Consider whether this person has legal obligations to protect the information – for example, is the person a covered entity required to comply with HIPAA, or a government employee or other person required to comply with other privacy laws? If so, there may be a lower probability that the PHI has been compromised. Also consider if the unauthorized person has the ability to re-identify the information.

Describe who used or received the PHI, and whether they have legal obligation to protect the PHI:

_____

_____

Factor C. Consider whether the PHI was actually acquired or viewed. If electronic PHI is involved, this may require a forensic analysis of the computer to determine if the information was accessed, viewed, acquired, transferred, or otherwise compromised.

Describe whether the PHI was actually acquired or viewed. If available, attach the forensic analysis report. Otherwise, include the forensic analysis with the findings report sent at the conclusion of the investigation.

_____

_____

Factor D. Consider the extent to which the risk to the PHI has been mitigated – for example, as by obtaining the recipient's satisfactory assurances that the PHI will not be further used or disclosed (through a confidentiality agreement or similar means) has been completely returned or the PHI has been/will be destroyed. Organizations should consider the extent and efficacy of the mitigation when determining the probability that the PHI has been compromised. Office for Civil Rights (OCR) notes that this factor, when considered in combination with the factor regarding the unauthorized recipient, may lead to different results in terms of the risk of PHI. For example, a provider may be able to obtain and rely on the assurances of an employee, affiliated entity, business associate, or another covered entity that the person destroyed the information. However, such assurances from other third parties may not be sufficient.

Describe risk mitigation steps taken:

_____

_____

Factor E. Describe any other relevant factors (write "none" if appropriate):

_____

_____

Based on the factors in the risk assessment noted above, is there a **LOW** probability that the PHI has been compromised?

☐ Yes, there is a low probability, thus NO breach reporting required under HIPAA.

☐ No, there is not a low probability, thus breach reporting is required under HIPAA.

IMPORTANT NOTE: This tool is helpful only with respect to a decision whether reporting is required under federal law (HIPAA). State laws may require notification of a breach as defined in state law regardless of the results of this risk assessment.

Signature of person completing this form: _____

Title: _____ Date: _____