|  |  |  |
| --- | --- | --- |
| **DEPARTMENT OF HEALTH SERVICES**  Division of Medicaid Services  F-02432 (10/2022) | | **STATE OF WISCONSIN** |
| **IRIS PROGRAM HIPAA BREACH AND UNAUTHORIZED DISCLOSURE REPORTING** | | |
| All completed requests should be submitted electronically to [DHSIRISContractCompliance@dhs.wisconsin.gov](mailto:DHSIRISContractCompliance@dhs.wisconsin.gov) with any and all attachments relevant to the investigation or resolution of the incident. | | |
| To protect individuals from the potential harm from the unauthorized disclosure or breach of protected health information (PHI) or personally identifiable information (PII), DHS requires timely and accurate communication. Immediately upon discovery of a suspected information breach and/or unauthorized disclosure of PHI or PII, please notify IRIS (IRIS Contract Compliance). **IRIS, in consultation with the DHS Privacy Officer, will determine and provide direction for subsequent steps, including notification of affected individuals, if necessary.**  **INSTRUCTIONS**: Please mark which notification this form represents. If this is an “initial notification” of a potential breach or unauthorized disclosure, please fill out with as much information known at the time. If this is a “final notification”, please update the original initial notification form with the rest of the information and resend with accompanying documents. Additionally, please include the date of the potential breach or unauthorized disclosure and whether it is an initial or final notification in the subject line of the email. | | |
|  | Initial Notification (fill out form best to ability) | |
|  | Final Notification (update Initial Notification form and resend to DHS) | |
| Agency Name | | Agency Reporter/HIPAA Compliance/Security Officer Name |
| Click here to enter text. | | Click here to enter text. |
| Work Phone | | Email Address |
| Click here to enter text. | | Click here to enter text. |
| Date of Discovery | | Date of Unauthorized Disclosure |
| Click here to enter a date. | | Click here to enter a date. |
| Name(s) of Impacted IRIS Participant(s) and/or IRIS Participant-Hired Worker(s) | | |
| Name(s) of those impacted by breach/unauthorized disclosure. | | |
| Number of Impacted IRIS Participant(s) and/or IRIS Participant-Hired Worker(s) | | |
| Add numbers. | | |
| Information disclosed or breached (select all that apply) | | |
| Name(s) of Participant or Legal decision maker | | MCI Number |
| Address | | Social Security Number |
| Phone Number | | Medical Information |
| Date of Birth | | IRIS and/or Medicaid Enrollment |
| Other: Details | | |
| How did the breach occur? (select all that apply) | | |
| Lost or Stolen Cell Phone | | Lost or Stolen Desktop Computer |
| Lost or Stolen Laptop | | Lost or Stolen Tablet |
| Email | | Phone |
| WISITS | | SFTP/FTP Site |
| Public Conversation | | Copies |
| Fax | | Mail |
| Other: Details | | |
| What confirmation, if any, was received from the recipient as to the return, destruction, or deletion of content received? | | |
| Confirmation details. | | |
| Incident Description (provide as much detail as possible; who, what, where, when, why, how): | | |
| Incident description. | | |
| Next Steps (action required by the ICA/FEA or DHS, timeline, etc.): | | |
| Click here to enter text. | | |
| Long-Term Mitigation Measures to Prevent Future Incidents: | | |
| Mitigation measures and strategy. | | |
| Additional Documents Provided | | |
| Notification Communication to Participant/PHW Involved in Breach (Requires DHS Approval | | |
| Breach Risk Assessment (if the decision is made not to notify the affected individuals, a risk assessment must be completed. See below) | | |
| Press Release (Draft) | | |
| Credit Monitoring Information | | |
| Other: Add details for other attached documents. | | |
| **ADDITIONAL IMPORTANT INFORMATION**  **Conducting a Risk Assessment:** An unauthorized acquisition, access, use, or disclosure of protected health information in a manner not permitted under the Privacy Rule is presumed to be a breach as defined in 45 CFR 164.402(2), unless the Department demonstrates through a Risk Assessment that there is a low probability that the protected health information has been compromised.   1. A Risk Assessment based on the following factors must be completed:    1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;    2. The unauthorized person who acquired, accessed, used, or disclosed the protected health information or to whom the disclosure was made;    3. Whether the protected health information was actually acquired or viewed; and    4. The extent to which the risk of compromise to the protected health information has been mitigated. 2. Evaluate the overall probability that the protected health information has been compromised by considering all the factors in their totality. If the evaluation of the factors fails to demonstrate the low probability the protected health information has been compromised. Breach notification is necessary and required.   **Breach Notification Requirements:** If it is determined that a breach has occurred based upon the results of a properly completed Risk Assessment, identify the individuals whose PHI has been compromised. These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of the breach pursuant to 45 CFR 164.404. A breach shall be treated as a discovered on the first day the breach is known, or by exercising reasonable diligence, would have been known. Time for notifications begins when a breach is discovered or should have been discovered | | |