BAY ARENA

CORPORATE COMPLIANCE
PRIVACY/BREACH RECORD

Date Complaint Received
Source of Complaint

Suspected Violation

Type of Provider
Name of Provider
- **Owner/Director**
- **Address**
- **Phone**

Consumer(s) Involved

BABH ID	Medicaid ID	Name

Communications

- ☐ Acknowledged w/in 5 business days
- ☐ CEO aware
- ☐ Recipient Rights Office aware
- ☐ Human Resources aware
- ☐ Supervisor aware
- ☐ Other:
- ☐ Logged

☐ not necessary
☐ not necessary
☐ not necessary
☐ not necessary
☐ not necessary

Record of Activity

Breach Determination

NOTE: Per the HITECH Act, all acquisition, access, use or disclosure of PHI not permitted under the privacy rule is presumed to be a breach unless an exception applies, or a risk assessment determines there is a low probability that the PHI has been compromised

Incident	Yes/No
Did an acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule occur?	
If there a data breach, the Security Officer must complete a Security Incident Worksheet	
If yes, is this incident excluded from the definition of a breach?	**Yes/No**
Unintentional acquisition, access or use of PHI by employee/workforce member Example- An employee/contracted LIP opens an e-mail containing PHI. The employee notices they are not the intended recipient, alerts the sender of the misdirected e-mail, and then deletes it.	
Inadvertent disclosure to another authorized person within the entity or OHCA	

Example- A contracted service provider w/ the authority to use or disclose PHI discloses it to another contracted service provider w/ the authority to use or disclose PHI; or a MSHN CMSHP discloses to another MSHN CMHSP	
Recipient could not reasonably have retained the data Example, a covered entity, due to a lack of reasonable safeguards, sends letters to the wrong individuals. A few letters are returned by the post office, unopened, as undeliverable. In these circumstances, the covered entity can conclude that the improper addressees could not reasonably have retained the information. Data is limited to limited data set that does not include dates of birth or zip codes.	
If 'Yes' is selected as an answer to one or more of the exception questions, a breach has not occurred If all of the questions are marked 'No' the Breach Risk Assessment must be completed	

Breach Risk Assessment

☐ **Not Applicable**

Method of Disclosure	**Risk Scale**	**Score**
View only	1	
Verbal only	1	
Paper only	2	
Electronic only	3	
Both paper and electronic	3	
Recipient of Disclosure	**Risk Scale**	**Score**
Employee/contracted LIP without need-to-know	1	
Contracted service provider agency without need-to-know	1	
Out of network covered entity	2	
Wrong payor/insurance company	2	
Unauthorized consumer or family member; employee family member, non covered entity	2	
Unknown recipient, lost or stolen	3	
General public, media, etc.	4	
Circumstances of Release	**Risk Scale**	**Score**
Unintentional disclosure	1	
Intentional use/access without authorization	2	
Intentional disclosure without authorization	2	
Loss or theft	2	
Using false pretense to obtain or disclose	3	
Obtain for personal gain or with malicious intent to cause harm	3	
Hacked/targeted data breach	3	
Disposition of Information	**Risk Scale**	**Score**
Original/complete information returned	1	
Information properly destroyed (written assurance obtained)	1	
Information could not reasonably be retained	1	
Information properly destroyed (NO assurance obtained)	2	
Electronically deleted	2	
Unable to retrieve/unsure of location/disposition	3	
High probability of re-disclosure or suspected re-disclosure	3	
Disclosed to media	3	
Type of Information	**Risk Scale**	**Score**
Limited data set/de-identified data	1	
Non-sensitive – demographic information with no financial or sensitive treatment. Example – date of service, provider, service description, service code, etc.	2	

First name or first initial, and last name, in combination with one of the following: • Social security number • Driver's license or state ID • Health insurance policy numbers • Information regarding medical history, diagnoses, treatment, etc. • Username, password and/or security question for online account	3	
An individual's first name or first initial, and last name, in combination with: • Sensitive PHI such as alcohol and drug use history/treatment, HIV status, etc. • More than one data element from Risk Level 3 (for Type of Information)	4	
Overall Level of Risk	**Total Score**	
Low 5-8, Low-Moderate 9, Moderate 10-12, Mod-High 13, High 14-17		
Acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule (for which a breach exception does not exist) is presumed to be a breach unless the risk is assessed to be Low. Notification is required.		

Breach Notification

☐ **Not Applicable**

☐ Notice to Affected Individuals
☐ MDHHS & MSHN
☐ Credit Bureaus
☐ Police Report
☐ Media
☐ US Dep't Health/Human Serv
☐ Website
☐ Other:
☐ Other:

Mitigation/Remediation Plan

☐ **Not Applicable**

1. Action Step:
   a. Status:

Completed by Janis Pinter LMSW, ACSW
Corporate Compliance & Privacy Officer
Director of Healthcare Accountability

Date 8/19/2021