Incident #_____ Program Office: _____ Completed by:

HIPAA RISK ASSESSMENT DECISION TREE
To Be Used in Determining Whether a HIPAA Privacy Breach Has Occurred

NOTE: ALL INCIDENTS, WHETHER RESULTING IN NOTIFICATION OR NOT, MUST BE REPORTED TO THE DCF OFFICE OF CIVIL RIGHTS

STEP	QUESTION	IF YES	IF NO	RESPONSE
Unsecured / Secured PHI				
1	Was there access, acquisition, use or disclosure of **UNSECURED** PHI in any form? ▪ Unsecured PHI - Unencrypted or improperly encrypted electronic PHI (ePHI) - Improperly disposed or destroyed paper, film, or other hard-copy PHI	Continue to Step 2	No Breach has occurred under Privacy Rule. Notifications not required. Document decision. **Report incident to Office of Civil Rights.**	
Specific Breach Definition Exclusions				
2	Was it an unintentional acquisition, access, use or disclosure by an employee acting under the Department's authority, made in good faith, within the scope of the employee's authority and did not result in further use/disclosure?	May make determination risk is low and not provide notifications. Document decision. **Report incident to Office of Civil Rights.**	Continue to Step 3	
3	Was it an inadvertent disclosure by a person with authority to access PHI to another person authorized to access PHI at the same organization ***and*** the information was not disclosed or used further?	May make determination risk is low and not provide notifications. Document decision. **Report incident to Office of Civil Rights.**	Continue to Step 4	
4	Was an unauthorized disclosure made, but there is a good faith belief that the recipient would not be able to reasonably retain the information (e.g. returned unopened or handed to wrong individual and immediately taken back before unauthorized recipient can read PHI)?	May make determination risk is low and not provide notifications. Document decision. **Report incident to Office of Civil Rights.**	Continue to Step 5	
Minimum Necessary Rule				
5	Did the access, use or disclosure involve more than the minimum necessary to accomplish the purpose?	Continue to Step 6	May make determination risk is low and not provide notifications. Document decision. **Report incident to Office of Civil Rights.**	

STEP	QUESTION	IF YES	IF NO	RESONSE
Does the impermissible use or disclosure compromise the security or privacy of the PHI?				
6	Was acquisition, access, use or disclosure unrelated to the employee's duties (e.g. case worker looks through family member's file to learn of services received)?	Risk High. Make notifications. **Report incident to Office of Civil Rights.**	Continue to Step 7	
7	Was it received and/or used by another entity governed by the HIPAA Privacy & Security Rules or a Federal Agency obligated to comply with the Privacy Act.	May make determination risk is low and not provide notifications. Document decision. **Report incident to Office of Civil Rights.**	Continue to Step 8	
8	Were immediate steps taken to mitigate an impermissible use/disclosure (e.g., Contact recipient and obtain their assurances that the information will be destroyed or not be disclosed any further)?	May make determination risk is low and not provide notifications. Document decision. **Report incident to Office of Civil Rights.**	Continue to Step 9	
9	Was the PHI returned prior to being accessed for an improper purpose (e.g., A laptop is lost/stolen, then recovered & forensic analysis shows the PHI was not accessed, altered, transferred or otherwise compromised)? *Do not delay notification if recovery is not immediate.*	May make determination risk is low and not provide notifications. Document decision. **Report incident to Office of Civil Rights.**	Continue to Step 10	
What type and amount of PHI was involved? What is the Likelihood of re-identification?				
10	Does the unauthorized acquisition, access, use or disclosure involve information that is more sensitive in nature? (e.g., Financial, sexually transmitted disease information, mental health information, substance abuse information, detailed clinical information, etc.)	Risk High. Provide notifications. **Report incident to Office of Civil Rights.**	Continue to Step 11	
11	Did the improper use/disclosure only include the client name and the fact that services have been provided by the Department (e.g. individual identified as being a DCF client)?	May make determination risk is low and not provide notifications. Document decision. **Report incident to Office of Civil Rights.**	Continue to Step 12	

STEP	QUESTION	IF YES	IF NO	RESSPONSE
12	Did the improper use/disclosure include the information increases the risk of ID Theft (such as SS#, date of birth, mother's maiden name)?	Risk High. Provide notifications. **Report incident to Office of Civil Rights.**	Continue to Step 13	
13	Was a limited data set [164.514(e)][i] or de-identified data [164.514(b)][ii] used or disclosed?	Continue to Step 14	Continue to Step 14	
14	Is the risk of re-identification [164.514(c)[iii] so small that the improper use/disclosure poses low risk of compromise to the security or privacy of the PHI?	May make determination risk is low and not provide notifications. Document decision. **Report incident to Office of Civil Rights.**	Risk High. Provide notifications. **Report incident to Office of Civil Rights.**	

[i] A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (i) Names; (ii) Postal address information, other than town or city, State, and zip code; (iii) Telephone numbers; (iv) Fax numbers;(v) Electronic mail addresses;(vi) Social security numbers; (vii) Medical record numbers; (viii) Health plan beneficiary numbers; (ix) Account numbers; (x) Certificate/license numbers; (xi) Vehicle identifiers and serial numbers, including license plate numbers; (xii) Device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) Biometric identifiers, including finger and voice prints; and (xvi) Full face photographic images and any comparable images.

[ii] Requirements for de-identification of protected health information. A covered entity may determine that health information is not individually identifiable health information only if:
(1) A person with appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods for rendering information not individually identifiable: (i) Applying such principles and methods determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information by an anticipated recipient to identify an individual who is a subject of the information; and (ii) Documents the methods and results of the analysis that justify such determination; or (2) (i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed: (A) Names. (B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000. (C) 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. (D) Telephone numbers. (E) Fax numbers. (F) Electronic mail addresses. (G) Social security numbers. (H) Medical record numbers. (I) Health plan beneficiary numbers. (J) Account numbers. (K) Certificate/license numbers. (L) Vehicle identifiers and serial numbers, including license plate numbers. (M) Device identifiers and serial numbers. (N) Web Universal Resource Locators (URLs). (O) Internet Protocol (IP) address numbers. (P) Biometric identifiers, including finger and voice prints. (Q) Full face photographic images and any comparable images. (R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and
(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

[iii] Re-identification. A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that: (1) Derivation. The code or other means of record identification is not derived from, or related to, information about the individual and is not otherwise capable of being translated so as to identify the individual; and (2) Security. The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.