

## COMPARATIVE HEALTH PRIVACY LAW MATRIX

This template has been developed to assist the State of Washington compare state and federal Health Information Privacy laws. Specifically, the matrix will assist with our pre-emption analysis of the Health Insurance Portability and Accountability Act (HIPAA). HIPAA sets a national “floor” or minimum level of privacy protection for health information. State law that sets a higher standard remains valid, while state law that sets a lower standard than HIPAA is superceded. Any state law that is both contrary to and more stringent than HIPAA must be submitted to the Secretary of HHS for a decision about which law prevails.

The Matrix is designed to be used as a template for comparison of other state’s laws to facilitate a national view, using the same categories, of where state law and HIPAA intersect. The matrix is currently divided into three sections, each containing a word table.

**INDEX:** The first table contains the standard categories or terms down the left side, and the citation to HIPAA and state law in the next columns. Once completed, the citations will be color coded (probably red, yellow, green) to indicate which state laws we believe are superceded by HIPAA and which state laws remain in effect.

**TERMS COMPARISON:** The second table lists the same standard categories, the HIPAA and state law citations, and brief descriptions of these provisions.

**CONTEXT SPECIFIC STATE LAW:** The third table contains state laws that are not comprehensive privacy laws, but have smaller or some provision related to health information privacy. This table is in alphabetic order by context specific information with HIPAA provision highlighted in the next column.

**FEDERAL LAW:** A fourth table may be added to compare additional federal law that contains comprehensive privacy protections. It will be laid out similar to Section two and may include such statutes and regulations related to HIV/AIDS records, mental health records, drug and alcohol treatment records, domestic violence records, and Medicaid participant records.

## Health Privacy Matrix - INDEX

| Term                                      | HIPAA Privacy<br>45 CFR §164                 | State Statute | State Administrative Code | Other State law |
|-------------------------------------------|----------------------------------------------|---------------|---------------------------|-----------------|
| <b>APPLICABILITY</b>                      |                                              |               |                           |                 |
| <b>Applicable Entity</b>                  | §160.102; 164.104; 500                       |               |                           |                 |
| <b>Applicable Information</b>             | §164.501                                     |               |                           |                 |
| <b>Applicable Individuals</b>             | §164.501; 502(f)(g)                          |               |                           |                 |
| <b>Minors</b>                             | §160.202; 164.502(g)                         |               |                           |                 |
| <b>USE AND DISCLOSURE RESTRICTIONS</b>    |                                              |               |                           |                 |
| <b>General</b>                            | §164.502(a)                                  |               |                           |                 |
| <b>Minimum Necessary</b>                  | §164.502(b)                                  |               |                           |                 |
| <b>De-Identified</b>                      | §164.514                                     |               |                           |                 |
| <b>Permitted - No Restrictions</b>        | §164.512                                     |               |                           |                 |
| <b>Permitted - Agree or Object</b>        | §164.510                                     |               |                           |                 |
| <b>Permitted - Consent Required</b>       | §164.506                                     |               |                           |                 |
| <b>Permitted - Authorization Required</b> | §164.508                                     |               |                           |                 |
| <b>Research</b>                           | §164.512                                     |               |                           |                 |
| <b>Marketing or Fundraising</b>           | 164.514(e) and (f)                           |               |                           |                 |
| <b>Required Disclosures</b>               | §164.502(a)(2)                               |               |                           |                 |
| <b>INDIVIDUAL RIGHTS</b>                  |                                              |               |                           |                 |
| <b>Individual Rights - General</b>        | §164.522                                     |               |                           |                 |
| <b>Right to Notices and other Forms</b>   | §164.520                                     |               |                           |                 |
| <b>Right to Access, Copy or Amend</b>     | §164.524; §164.526                           |               |                           |                 |
| <b>Right to Audit or Accounting</b>       | §164.528                                     |               |                           |                 |
| <b>Waiver</b>                             | §164.530(h)                                  |               |                           |                 |
| <b>ADMINISTRATIVE REQUIREMENTS</b>        |                                              |               |                           |                 |
| <b>General Privacy Standard</b>           | §164.530(l)(l)                               |               |                           |                 |
| <b>Provide Notice and Forms</b>           | §164.530(j); §164.506;<br>§164.508; §164.520 |               |                           |                 |
| <b>Personnel Requirements</b>             | §164.530(a); (b); (e)                        |               |                           |                 |
| <b>Policies and Procedures</b>            | §164.530(l)                                  |               |                           |                 |
| <b>Safeguards</b>                         | §164.530(c)                                  |               |                           |                 |
| <b>Business Associates</b>                | §164.502(e); 164.504(e)                      |               |                           |                 |
| <b>Security and Destruction</b>           | §164.514(H)                                  |               |                           |                 |
| <b>Documentation and Retention</b>        | §164.530(d)                                  |               |                           |                 |
| <b>REMEDIES AND PENALTIES</b>             |                                              |               |                           |                 |
| <b>Complaints - Internal</b>              | §164.530(d)                                  |               |                           |                 |
| <b>Complaints - Other</b>                 | §160.306                                     |               |                           |                 |
| <b>Enforcement and Sanctions</b>          | Future and Statute                           |               |                           |                 |
| <b>Private Right of Action</b>            | None                                         |               |                           |                 |



| Term                          | HIPAA Privacy Regulation<br>45 CFR §164                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |  |  |  |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|
| APPLICABILITY                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |  |  |  |
| <b>Applicable Entity</b>      | <p>§160.102; 164.104; 500.<br/>Applies to Covered Entities (CE): health care providers that conduct electronic transactions, health plans, and clearinghouses.</p> <p>Providers broadly defined: provider of medical or health care services; or is paid for health care services/supplies in normal course of business.</p> <p>Health Plan is any group that provides or pays the cost of medical care (with some exceptions for government programs).</p> <p>Clearinghouses perform data translation and other services on behalf of providers, plans and others.</p> <p>CE's must also pass on requirements to business associates (BA) through contracts. BA's are not directly regulated.</p> |  |  |  |
| <b>Applicable Information</b> | <p>§164.501. Any information created or received by or on behalf of the CE that identifies or reasonably could be used to identify an individual; and relates to health condition, care or payment.</p> <p>Applies to information in any</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                       |  |  |  |

| Term                                   | HIPAA Privacy Regulation<br>45 CFR §164                                                                                                                                                               |  |  |  |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|
|                                        | form, including oral. Protected health Information (PHI) excludes educational records governed by FERPA. §164.508 Psychotherapy notes are subject to authorization.                                   |  |  |  |
| <b>Applicable Individuals</b>          | §164.501, 502(f)(g). Any individual person who is the subject of protected health information, whether alive or deceased. Allows for personal representative to act on the individual's behalf.       |  |  |  |
| <b>Applicable to Minors</b>            | §160.202; 164.502(g). Defers to State Law. Allows parent or guardian to act as personal representative.                                                                                               |  |  |  |
| <b>USE AND DISCLOSURE RESTRICTIONS</b> |                                                                                                                                                                                                       |  |  |  |
| <b>General</b>                         | §164.502(a). Generally, CE cannot use or disclose PHI except pursuant to a consent, authorization, or specific exception.                                                                             |  |  |  |
| <b>Minimum Necessary</b>               | §164.502(b). CE may only use or disclose the minimum amount of information that is necessary to accomplish the purpose or task.<br>§164.514(d) details implementation specifications for minimum use. |  |  |  |
| <b>De-identified Information</b>       | §164.514. De-identified information is not subject to                                                                                                                                                 |  |  |  |

| Term                                            | HIPAA Privacy Regulation<br>45 CFR §164                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |  |  |  |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|
|                                                 | <p>restrictions. Extremely specific: must have statistical analyst certify not likely to re-identify or the following identifiers removed: names, geographical subdivisions smaller than a state (first three digit zipcode with population over 20,000 ok); all elements of date except year; telephone number; fax number; email; social security number; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers; devise identifiers; URLs; IP address numbers; biometric identifiers; full face photo image; and nay other unique identifying number, code.<br/>Re-identification codes are PHI.</p> |  |  |  |
| <b>Permitted -No Restrictions by Individual</b> | <p>§165.512. CE may disclose without consent, authorization, or opportunity to agree or object by the individual for following uses, but specific limitations may apply:<br/>Uses and disclosures <u>required</u> by law; Uses and disclosures for public health activities;<br/>Disclosures about victims of abuse, neglect or domestic violence; Uses and disclosures for health oversight activities;<br/>Disclosures for judicial and administrative proceedings;<br/>Disclosures for law enforcement</p>                                                                                                                                                               |  |  |  |

| Term                                                     | HIPAA Privacy Regulation<br>45 CFR §164                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |  |  |  |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|
|                                                          | <p>purposes; Uses and disclosures about decedents; Uses and disclosures for cadaveric organ, eye, or tissue donation purposes; Uses and disclosures for research purposes; Uses and disclosures to avert a serious threat to health or safety; Uses and disclosures for specialized government functions; and Disclosures for workers compensation.</p>                                                                                                                                                                                                                                                                                                                                               |  |  |  |
| <p><b>Permitted - Opportunity to Agree or Object</b></p> | <p>§164.510<br/>A CE may use or disclose IIHI, provided the individual has an opportunity to agree or object to the use or disclosure for the following purposes:</p> <ul style="list-style-type: none"> <li>▪ Use and disclosure for a facility directory;</li> <li>▪ Disclosures to a friend or relative that the individual has identified as being involved with the individual's health care or payment for the health care;</li> <li>▪ Uses and disclosures for notification of the individual's locations, condition or death to a family member, personal representative, or another person responsible for the care of the individual.</li> </ul> <p>If the individual is not present or</p> |  |  |  |

| Term                                             | HIPAA Privacy Regulation<br>45 CFR §164                                                                                                                                                                                                                                                                                                                                                                                         |  |  |  |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|
|                                                  | <p>unable to agree or object due to incapacity or an emergency situation, the covered entity may disclose information directly related to the person's involvement in the individual's care. The disclosure must be determined, in the professional judgement of the covered entity, to be in the individual's best interest.</p>                                                                                               |  |  |  |
| <p><b>Permitted - Consent Required</b></p>       | <p>§164.506<br/>CE may use or disclose information for treatment, payment of health care operations (TPO).<br/>Providers must obtain a consent for use and disclosures for TPO but can condition treatment or enrollment on consent. Consent is valid until revoked. Consent must refer to Notice of Privacy practices.<br/>Plans and clearinghouses are not required to obtain a consent for uses and disclosures for TPO.</p> |  |  |  |
| <p><b>Permitted - Authorization Required</b></p> | <p>§164.508. The individual can authorize to release to anyone for any reason.<br/>CE must obtain authorization to use or disclose PHI for any other purpose. CE cannot condition treatment or enrollment on authorization. CE must follow detailed requirements for valid authorization.<br/>Psychotherapy notes disclosure</p>                                                                                                |  |  |  |

| Term                            | HIPAA Privacy Regulation<br>45 CFR §164                                                                                                                                       |  |  |  |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|
|                                 | require authorization.                                                                                                                                                        |  |  |  |
| <b>Research</b>                 | §164.512(i) CE may use or disclose for research subject to limitations. CE may obtain authorization, or receive a Board approval of a waiver, or IRB or privacy board review. |  |  |  |
| <b>Marketing or Fundraising</b> | §164.514(e)(1) and (f)(1). Generally requires the authorization of individual.                                                                                                |  |  |  |
| <b>Required Disclosures</b>     | §164.502(a) CE must disclose information to the individual or personal representative and to the Secretary of HHS for compliance investigations.                              |  |  |  |

| Term                                    | HIPAA Privacy Regulation<br>45 CFR §164                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |  |  |  |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|
| <b>Individual Rights - General</b>      | <p>§164.522. Individual has right to request restriction on use and disclosures. CE can refuse, but if agrees must abide.</p> <p>Individual has a right to request communication by alternative means or location.</p>                                                                                                                                                                                                                                                                                                                                    |  |  |  |
| <b>Right to Notices and other Forms</b> | <p>§164.520. Individual has a right to receive notice of information practices detailing the CE's use and disclosure of information.</p> <p>Individual rights re: consent and authorization, see above.</p> <p>All forms have specific requirements.</p>                                                                                                                                                                                                                                                                                                  |  |  |  |
| <b>Right to Access, Copy or Amend</b>   | <p>§164.524. Individual has right to access designated record (DRS) set as long as CE retains.</p> <p>Individual has a right to access and copy DRS.</p> <p>§164.526. Individual can request amendment to the DRS. CE must respond within 60 days by 1)amend inaccurate or incomplete data or determine record complete and accurate and notify individual. CE must have procedures for review. CE must also attempt to notify others of amendment who the individual requests or who may rely on the information to the detriment of the individual.</p> |  |  |  |
| <b>Right to Audit</b>                   | §164.528 Right to accounting of                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |  |  |

| Term                               | HIPAA Privacy Regulation<br>45 CFR §164                                                                                                                                                                                                                                                              |  |  |  |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|
| <b>or Accounting</b>               | disclosures by or on behalf of CE for up to six years. Exceptions for accounting include disclosures for treatment, payment, operations, to individual, and others.                                                                                                                                  |  |  |  |
| <b>Waiver</b>                      | §164.530(b). CE may not require an individual to waive their rights under HIPAA in order to receive services.                                                                                                                                                                                        |  |  |  |
| <b>ADMINISTRATIVE REQUIREMENTS</b> |                                                                                                                                                                                                                                                                                                      |  |  |  |
| <b>General Privacy Standard</b>    | §164.530(i)(I). CE must develop and implement policies and procedures relating to PHI that are designed to comply with the privacy regulations. The policies and procedures must take into account the size of and the type of activities that relate to PHI undertaken.                             |  |  |  |
| <b>Provide Notice and Forms</b>    | <p>§164.520 CE must display notice of information use and disclosures prominently and copy given to patient or enrollee.</p> <p>There are specific requirements for the content and form of the notice.</p> <p>See above for consent, authorization, and other form conditions and requirements.</p> |  |  |  |
| <b>Personnel Requirements</b>      | <p>§164.530(a). Designate a privacy official responsible for implementation and a contact person to receive complaints and provide information.</p> <p>§164.530(b). Train all</p>                                                                                                                    |  |  |  |

| Term                           | HIPAA Privacy Regulation<br>45 CFR §164                                                                                                                                                                                                                                                                                                                                                       |  |  |  |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|
|                                | employees about Privacy policy and procedures.<br>§164.530(e). Develop and apply sanctions against employees who fail to comply.                                                                                                                                                                                                                                                              |  |  |  |
| <b>Policies and Procedures</b> | §164.530(i). Must implement reasonable policies and procedures designed to comply with regulations and revise or eliminate non-compliant policies. If policies changed, must comply with Notice of Privacy Practices requirements.                                                                                                                                                            |  |  |  |
| <b>Safeguards</b>              | §164.530(c). Must have appropriate administrative, technical, and physical safeguards to protect the privacy of PHI and reasonably safeguard PHI from any intentional or unintentional use of disclosure, or violation of the requirements of the regulation.                                                                                                                                 |  |  |  |
| <b>Business Associates</b>     | §164.502(e); §164.504(e)<br>Business associates (BA) are individual or entities that carry out a function on or behalf of the CE. CE must have reasonable assurances in the form of a contract or interagency agreement with business associates containing specified provisions relating to protection of PHI. CE must also document mitigation or sanction policies and actions against BA. |  |  |  |
| <b>Security and</b>            | §164.514(d-h) CE must have                                                                                                                                                                                                                                                                                                                                                                    |  |  |  |

| Term                                 | HIPAA Privacy Regulation<br>45 CFR §164                                                                                                                                                                                                                                                                                                                             |  |  |  |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|
| <b>Destruction</b>                   | verification procedures, establish administrative and physical safeguards, component barriers within the organization, and establish policy which may include role based access, for compliance with minimum use. Additional security provisions will be outlined in a separate security regulation. Destruction requirements for BA's are detailed in BA provision |  |  |  |
| <b>Documentation and Retention</b>   | §164.530. Compliance designations and policies must be documented and retained for six years from date of creation or effect. Also maintain consents, authorizations, disclosures, amendments, and alternative communication requests.                                                                                                                              |  |  |  |
| <b>REMEDIES AND PENALTIES</b>        |                                                                                                                                                                                                                                                                                                                                                                     |  |  |  |
| <b>Internal Complaint Procedures</b> | §164.530(d) CE must have and notify individuals of right to complain/ procedure Must have policy protecting individual against retaliation.                                                                                                                                                                                                                         |  |  |  |
| <b>Other Complaint Procedures</b>    | §160.306 Individual can complain to Secretary of HHS or enforcement designee (OCR) of HIPAA violations.                                                                                                                                                                                                                                                             |  |  |  |
| <b>Enforcement and Sanctions</b>     | 42 USC 1320(d) Significant civil and criminal penalties may be imposed for each violation. Secretary of HHS may audit for compliance. Federal funds may be at risk for non-compliance.                                                                                                                                                                              |  |  |  |

| Term                           | HIPAA Privacy Regulation<br>45 CFR §164                         |  |  |  |
|--------------------------------|-----------------------------------------------------------------|--|--|--|
| <b>Private Right of Action</b> | None explicitly given. HIPAA could be used as standard of care. |  |  |  |

### Context Specific State Requirements

| Context                                 | State Law Cite and Requirement | HIPAA Privacy Provision Implication                                                                                 |
|-----------------------------------------|--------------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>Adoption</b>                         |                                |                                                                                                                     |
|                                         |                                |                                                                                                                     |
|                                         |                                |                                                                                                                     |
| <b>Cancer Registry Disclosure</b>       |                                |                                                                                                                     |
| <b>Cancer Registry Reporting</b>        |                                | §165.512. CE may disclose without consent if required by law; or uses and disclosures for public health activities. |
| <b>Child Abuse</b>                      |                                |                                                                                                                     |
| <b>Child Support and Paternity Test</b> |                                |                                                                                                                     |
| <b>Civil Commitment</b>                 |                                |                                                                                                                     |
|                                         |                                |                                                                                                                     |
| <b>Communicable Disease Records</b>     |                                |                                                                                                                     |
| <b>Communicable Disease Reporting</b>   |                                |                                                                                                                     |
|                                         |                                |                                                                                                                     |
| <b>Drug and Alcohol Abuse Treatment</b> |                                |                                                                                                                     |
|                                         |                                |                                                                                                                     |
| <b>Elder Abuse</b>                      |                                |                                                                                                                     |
|                                         |                                |                                                                                                                     |
|                                         |                                |                                                                                                                     |
|                                         |                                |                                                                                                                     |
| <b>HIV/AIDS</b>                         |                                |                                                                                                                     |
| <b>Hospital Patient Records</b>         |                                |                                                                                                                     |
|                                         |                                |                                                                                                                     |
|                                         |                                |                                                                                                                     |
| <b>Local Health Department Records</b>  |                                |                                                                                                                     |
|                                         |                                |                                                                                                                     |

| Context                                   | State Law Cite and Requirement | HIPAA Privacy Provision Implication           |
|-------------------------------------------|--------------------------------|-----------------------------------------------|
| <b>Long Term Care Ombudsman</b>           |                                |                                               |
|                                           |                                |                                               |
| <b>Mental Health: Children</b>            |                                |                                               |
| <b>Mental Health: Adult</b>               |                                |                                               |
|                                           |                                |                                               |
|                                           |                                |                                               |
|                                           |                                |                                               |
|                                           |                                |                                               |
| <b>Minors – Emancipated</b>               |                                |                                               |
| <b>Minors – Out of Home Placement</b>     |                                |                                               |
|                                           |                                |                                               |
|                                           |                                |                                               |
|                                           |                                |                                               |
|                                           |                                |                                               |
|                                           |                                |                                               |
| <b>Sexually Transmitted Disease Tests</b> |                                |                                               |
|                                           |                                |                                               |
| <b>Tuberculosis</b>                       |                                |                                               |
|                                           |                                |                                               |
|                                           |                                |                                               |
|                                           |                                |                                               |
|                                           |                                |                                               |
| <b>Worker’s Compensation Claims</b>       |                                | N/A – Workers Compensation exempt from HIPAA. |