





<div>  <b>FUTURE OF PRIVACY FORUM</b> </div> <div> <b>Comparison of Consumer Health Privacy Frameworks: New York, Washington, and Connecticut</b> </div>			
New York Health Information Privacy Act	Washington My Health My Data	Connecticut SB 3	FPF Analysis
Reference			
<a href="#">Senate Bill 929, 2025 Reg. Sess (N.Y. 2025)</a>  Passed: January 22, 2025; not yet signed into law.	<a href="#">Washington Revised Code, title 19, chapter 373.</a>  Enacted: April 27, 2023 Effective: March 31, 2024 for most regulated entities; June 30, 2024 for small businesses.	<a href="#">Connecticut General Statutes chapter 743j</a> → <a href="#">2024 Supplement</a>  Enacted: June 26, 2023 Effective: October 1, 2023	The New York Health Information Privacy Act passed the state legislature on January 22. The NYHIPA has a similar scope and scale as Washington State's landmark My Health My Data Act (MHMD). This chart compares these frameworks as well as Connecticut's consumer health data protections in its comprehensive privacy law, which offers a third distinct model. This comparison does not include Nevada's SB 370 due to that law's similar scope and structure to MHMD and this law's focus on comparing frameworks.
Covered Data			
<p><b>"Regulated health information"</b> [RHI] is "any information that is reasonably linkable to an individual, or a device, and <b>is collected or processed in connection with the physical or mental health of an individual.</b>" § 1120(2). The definition specifies that <b>"location or payment information</b> that relates to an individual's physical or mental health <b>or any inference</b> drawn or derived about an individual's physical or mental health that is reasonably linkable to an individual, or a device, shall be considered, without limitation, [RHI]."</p> <p><b>Excludes:</b> "deidentified information" § 1120(2); Information processed by government entities and certain HIPAA and clinical trial data. § 1126.</p>	<p><b>"Consumer health data"</b> is "personal information that is linked or reasonably linkable to a consumer and <b>that identifies the consumer's past, present, or future physical or mental health status.</b>" MHMD provides an inclusive list of <b>12 examples of types of data that constitute "physical or mental health status,"</b> such as "Bodily functions, vital signs, symptoms"; "Biometric data"; "Genetic data"; and "Precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies" Wash. Rev. Code § 19.373.010(8).</p> <p><b>Excludes:</b> HIPAA-covered protected health information and information originating from a HIPAA-covered entity or business associate; personal information covered by GLBA, FCRA, and FERPA; "Deidentified data"; Data used for public or peer-reviewed research in the public interest; and "Publicly available information." Wash. Rev. Code §§ 19.373.010(18) &amp; 19.373.100 (1).</p>	<p><b>"Consumer health data"</b> means any personal data [i.e., "information that is linked or reasonably linkable to an identified or identifiable individual"] that <b>"a controller uses to identify a consumer's physical or mental health condition or diagnosis, and includes, but is not limited to, gender-affirming health data and reproductive or sexual health data."</b></p> <p>Consumer health data is a category of <b>"sensitive data."</b></p> <p><b>Excludes:</b> "de-identified data" and "publicly available information."</p> <p>Conn. Gen. Stat. § 42-515 (2024).</p>	<p>New York defines covered data broadly, similar to Washington, but the New York standard may be both broader and narrower than Washington in certain ways. Connecticut has the narrowest definition as it focuses on a controller's subjective intent to identify health conditions and diagnoses.</p> <p>» <b>Intent -- Unclear:</b> New York regulates information collected or processed <b>"in connection with"</b> physical or mental health. Washington's law, in contrast, covers data that <b>"identifies"</b> health status. Connecticut has the narrowest standard, as it has an intent requirement—it covers personal data that a controller <b>"uses to identify"</b> physical or mental health condition or diagnosis. It is unclear whether New York's standard is broader than Washington's. "In connection with" could be a lower standard than "identifies," or it could be read to require intent on the regulated entity's part.</p> <p>» <b>Fewer Carve-outs:</b> New York contains no explicit carveout for public data, nor does it exclude GLBA-covered entities or data. Failing to carve-out GLBA-covered entities or data could create significant compliance obligations for payment processors and other organizations who handle payment information. New York's exception for research is constrained to information collected as part of a clinical trial. As discussed below (see "Protected Individuals"), New York also does not exclude employee data.</p> <p>» <b>No Examples:</b> New York does not provide a list of examples of covered data, which makes it difficult to know what is in scope. For example, Washington's law includes "biometric" data, which is not typically considered health information, and information about "bodily functions." It is unclear whether either of these categories are covered by New York's definition.</p>
Protected Individuals			
<p><b>"Individuals," which is undefined.</b></p> <p>Unlike most state consumer privacy laws, NYHIPA's protections extend to <b>"individuals,"</b> which, due to the absence of typical qualifiers for jurisdiction and role, includes (a) <b>employees</b> and people who are acting in more than just their individual, personal capacity; and (b) residents of states other than New York. § 1120 (2) &amp; (4).</p>	<p><b>"Consumer"</b> means a natural person who acts only in an individual or household context and who is a—</p> <ul style="list-style-type: none"> <li>• Washington resident; or</li> <li>• Person whose consumer health data is collected [processed] in Washington.</li> </ul> <p><b>Excludes:</b> Individuals acting in an employment context.</p> <p>Wash. Rev. Code § 19.373.010(7).</p>	<p><b>"Consumer"</b> means an individual who is a <b>resident of Connecticut.</b></p> <p><b>Excludes:</b> Individuals acting in a <b>commercial / employment context</b> (e.g., employee "whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit or government agency").</p> <p>Conn. Gen. Stat. § 42-515(8) (2024).</p>	<p>» <b>Broad Applicability Beyond New York Residents:</b> New York's law is relevant to a much broader range of people than either Washington's or Connecticut's, because—</p> <ul style="list-style-type: none"> <li>• it is not limited by territoriality (e.g., it protects individuals who enter New York and individuals whose regulated health information is processed by a regulated entity located in New York); and</li> <li>• it likely applies to employees, not just consumers acting in their individual or household capacity, which likewise expands the scope of covered data.</li> </ul>

 <b>Comparison of Consumer Health Privacy Frameworks: New York, Washington, and Connecticut</b>			
New York Health Information Privacy Act	Washington My Health My Data	Connecticut SB 3	FPF Analysis
Covered Entities			
<p><b>"Regulated entities"</b> are those that either control the processing of regulated health information of a New York resident or someone physically present in New York, or an entity that is located in New York and controls the processing of regulated health information of an individual. § 1120(4).</p> <ul style="list-style-type: none"> <li>• <b>Excludes:</b> HIPAA covered entities. § 1126(3).</li> </ul> <p><b>"Service provider"</b> means any person or entity that processes RHI on behalf of a regulated entity. Service providers may also, in certain processing contexts, qualify as a regulated entity. § 1120(6).</p>	<p><b>"Regulated entity"</b> means legal entities who (a) conduct business in Washington or produce or provide products or services targeted to Washington consumers and (b) alone or jointly determine the "purpose and means of collecting, processing, sharing, or selling" of consumer health data. Regulated entities include <b>"small businesses."</b></p> <ul style="list-style-type: none"> <li>• <b>Excludes:</b> Government agencies, tribal nations, or contracted service providers who process consumer health data on a government agency's behalf.</li> </ul> <p><b>"Processor"</b> means that a person that processes consumer health data on behalf of a regulated entity.</p> <p>Wash. Rev. Code §§ 19.373.010(21) &amp; (23).</p>	<p><b>"Consumer health data controller"</b> includes "any controller [i.e., "a person who, alone or jointly with others, determines the purpose and means of processing personal data"] that, alone or jointly with others, determines the purpose and means of processing consumer health data."</p> <p><b>"Processor"</b> means a person who processes personal data on behalf of a controller.</p> <p>Consumer health data controllers may also be subject to additional obligations under the law if they meet the applicability thresholds in Conn. Gen. Stat. § 42-516 (i.e., (1) control or process the personal data of at least 100K consumers or (2) control or process the personal data of at least 25K consumers and derived more than 25% of their gross revenue from selling personal data).</p> <p>Conn. Gen. Stat. § 42-515 (2024).</p>	<p>» <b>New York has the Broadest Coverage:</b> New York will bring in more regulated entities under its scope, given that any business can become a covered entity if an individual physically enters New York.</p> <p>» <b>No Small Business Exemption:</b> Neither New York nor Washington exclude small businesses. Connecticut's provisions specific to consumer health data controllers apply to small businesses, whereas its broader obligations for "controllers" have narrower applicability.</p>
Permissible Purposes			
<p>Regulated entities must obtain <b>valid authorization</b> to process RHI <b>unless strictly necessary</b> for one of the following specified purposes:</p> <ul style="list-style-type: none"> <li>• Providing a product or service requested by the individual;</li> <li>• Internal business operations, excluding "any activities related to marketing, advertising, research and development, or providing products or services to third parties";</li> <li>• Thwarting "malicious, fraudulent, or illegal activity";</li> <li>• Detecting, responding to, or preventing security incidents or threats;</li> <li>• Protecting vital interests of the individual or the public interest in the area of health;</li> <li>• Preparing for/asserting legal claims; and</li> <li>• Complying with legal obligations. § 1122(1)(b)(ii).</li> </ul>	<p>Regulated entities are prohibited from:</p> <ul style="list-style-type: none"> <li>• <b>collecting</b> (defined broadly to include processing) consumer health data unless: <ul style="list-style-type: none"> <li>▸ With consent from the consumer for the collection "for a specified purpose"; or</li> <li>▸ "necessary to provide a product or service" requested by the consumer;</li> </ul> </li> <li>• <b>sharing</b> consumer health data unless: <ul style="list-style-type: none"> <li>▸ With consent from the consumer that is "separate and distinct" from the consent to collect consumer health data; or</li> <li>▸ "necessary to provide a product or service" requested by the consumer;</li> </ul> </li> <li>• <b>selling</b> consumer health data unless the entity obtains <b>"valid authorization."</b></li> <li>• <b>collecting, using, or sharing additional categories of consumer</b> health data, or consumer health data for additional purposes, not disclosed in their consumer health data privacy policies without: <ul style="list-style-type: none"> <li>▸ first disclosing the additional categories or purposes; and</li> <li>▸ obtaining the consumer's consent prior to such collection, use, or sharing.</li> </ul> </li> </ul> <p>Wash. Rev. Code §§ 19.373.020(1)(c)-(d), 19.373.030(1) &amp; 19.373.070(1).</p>	<p>Consumer health data controllers must obtain a consumer's <b>consent</b> before <b>selling, or offering to sell, consumer health data.</b></p> <p>Consumer health data controllers who are subject to the main requirements of the Act (i.e., are controllers who meet the applicability thresholds) must also:</p> <ul style="list-style-type: none"> <li>• Limit the <b>collection of personal data</b> to what is adequate, relevant and reasonably necessary in relation to the disclosed purposes for which such data is processed;</li> <li>• Not "process personal data for purposes that are neither <b>reasonably necessary to, nor compatible with</b>, the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's <b>consent</b>"; and</li> <li>• Controllers must get <b>consent</b> for processing <b>sensitive data</b>, which includes "consumer health data" and "data revealing . . . mental or physical health condition or diagnosis."</li> </ul> <p>The Act maintains several broad exemptions, including for conducting internal research for product improvement and performing internal operations that are reasonably aligned with the expectations of the consumer.</p> <p>Conn. Gen. Stat. §§ 42-520, 42-524 &amp; 42-526.</p>	<p>New York provides a broader array of permissible processing purposes which do not require authorization. Whereas MHMD requires consent for any collection or sharing that is not necessary to provide a requested product or service, New York includes a list of other activities that do not require authorization (e.g., internal business operations). However, New York's "strictly necessary" standard may be less permissive than Washington's "necessary" standard.</p> <p>New York's consent requirements are much stricter than MHMD. In New York, strict "valid authorization" is required for any RHI processing outside a permissible purpose. In contrast, MHMD, has a two-tier consent standard, "consent" and stricter "valid authorization" solely for the sale of covered data. For a comparison of valid authorization requirements, see below.</p> <p>Connecticut has the fewest restrictions on how entities can collect and use consumer health data. Like New York and Washington, it includes restrictions on selling such data absent consumers' consent. If an entity is a controller, then it must obtain consent prior to processing consumer health data for any non-exempt processing purposes. Connecticut does not, however, include any kind of "necessary" or "strictly necessary" data minimization requirement limiting collection and processing of sensitive data to what is needed to provide a requested product or service.</p>

<div>  <div> <div>Comparison of Consumer Health Privacy Frameworks:</div> <div>New York, Washington, and Connecticut</div> </div> </div>			
New York Health Information Privacy Act	Washington My Health My Data	Connecticut SB 3	FPF Analysis
Consent / Authorization Requirements			
<p>To <b>sell</b> or <b>process</b> RHI for any reason not "strictly necessary" to those listed, regulated entities must obtain <b>"valid authorization."</b> A request for authorization must be—</p> <ul style="list-style-type: none"> <li>• Signed by the consumer;</li> <li>• Made separately from any other transaction or part of a transaction;</li> <li>• Made <b>"at least twenty-four hours after</b> an individual creates an account or first uses the requested product or service";</li> <li>• If multiple categories of processing are involved, provide an ability to "provide or withhold" authorization for each category separately; and</li> <li>• Include required information, such as types of RHI to be processed, the nature and specific purposes of processing, the names or categories of service providers and third parties to whom RHI is disclosed (as well as the purposes for disclosure), consideration the regulated entity may receive in connected with processing RHI, and an expiration date (maximum of one-year). § 1122(2).</li> </ul> <p><b>Note:</b> Due to drafting ambiguity, there is a plausible reading of 1122(a) that prohibits selling RHI without allowing for doing so pursuant to valid authorization.</p>	<p>To <b>sell</b> consumer health data, regulated entities must obtain separate <b>"valid authorization"</b> that is—</p> <ul style="list-style-type: none"> <li>• Signed by the consumer;</li> <li>• Separate and distinct from any consent obtained to collect or share consumer health data;</li> <li>• Includes required information, such as the name and contact information of the person purchasing the data, the purpose of the sale (including how the data will be used by the purchaser), and a one-year expiration date;</li> <li>• Is not combined with other documents to create a "compound authorization"; and</li> <li>• Does not condition the provision of goods or services on the consumer signing a valid authorization.</li> </ul> <p>Wash. Rev. Code § 19.373.070.</p> <p>MHMD also requires a separate form of "consent" for processing activities that are not necessary to provide a requested product or service. <b>"Consent"</b> is a "clear affirmative act that signifies a consumer's freely given, specific, informed, opt-in, voluntary, and unambiguous agreement." Consent is revocable. Wash. Rev. Code §§ 19.373.010(6) &amp; 19.373.040(1)(b).</p>	<p><b>"Consent"</b> is "a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to allow the processing of personal data relating to the consumer." Consent is revocable. Conn. Gen. Stat. §§ 42-515(7) &amp; 42-520 (2024).</p> <p>Consumer health data controllers must obtain a consumer's <b>consent</b> before <b>selling, or offering to sell, consumer health data</b>. Conn. Gen. Stat. § 42-526 (2024).</p> <p>Consumer health data controllers who are controllers under the Act must obtain <b>consent</b> for <b>processing sensitive data</b>, which includes "consumer health data" and "data revealing . . . mental or physical health condition or diagnosis." Conn. Gen. Stat. § 42-520(a) (2024).</p>	<p>» <b>New York Has the Most Restrictive Consent Requirements:</b> New York's authorization scheme is simpler than Washington's two-tier standard, which requires "consent" for some collection and sharing of consumer health data but requires "valid authorization" for selling such data.</p> <p>For processing activities and sharing of data other than sales, however, New York's authorization requirements are much stricter than Washington's consent requirements, both in terms of procedural requirements (e.g., 24 hour waiting period) and the content of requests. When it comes to selling data, the valid authorization requirements for the two regimes are similar in scope and content, although New York's 24 hour waiting period is still unique.</p> <p>» <b>Connecticut is Simplest:</b> Connecticut has easiest consent requirements to implement, as it requires the freely given, specific, informed, and unambiguous consent that is typical of U.S. state privacy laws and many privacy laws globally and does not require a different, stricter kind of consent (valid authorization) for selling consumer health data.</p>
Individual Rights			
<p>New York grants individuals:</p> <ul style="list-style-type: none"> <li>• The <b>right to access</b> their regulated health information through an "effective, efficient, and easy-to-use mechanism" within 30 days of receiving a request. § 1123(1)(a).</li> <li>• The <b>right to immediately revoke authorization</b> for processing at any time via an "effective, efficient, and easy-to-use mechanism." § 1122(2)(c).</li> <li>• The <b>right to delete</b> their regulated health information within 30 days. § 1123(2). <ul style="list-style-type: none"> <li>› Upon receiving a deletion request a regulated entity shall <b>notify</b> "each service provider or third party that processed the individual's [RHI] in connection with a transaction involving the regulated entity occurring within one year preceding the individual's request" unless it is "impossible or involves disproportionate effort that is documented in writing." § 1123(2)(c)(ii).</li> <li>› Deletion or cancellation of an online account "shall be treated as a request to delete [RHI]." § 1123(2)(b).</li> </ul> </li> </ul>	<p>MHMD grants individuals:</p> <ul style="list-style-type: none"> <li>• The <b>right to confirm</b> whether a regulated entity is collecting, sharing, or selling their consumer health data;</li> <li>• The <b>right to access</b> their consumer health data (including to whom their consumer health data was shared or sold);</li> <li>• The <b>right to withdraw consent</b> for the collection or sharing of their consumer health data; and</li> <li>• The <b>right to delete</b> their consumer health data. Regulated entities that receive deletion requests from individuals must: <ul style="list-style-type: none"> <li>› <b>Delete</b> that consumer's consumer health data from all of its records, including archived or backup systems; and <b>Notify</b> "all affiliates, processors, contractors, and other third parties with whom the regulated entity . . . has shared consumer health data of the deletion request."</li> </ul> </li> </ul> <p>Wash. Rev. Code § 19.373.040.</p>	<p>Connecticut has no rights specific to consumer health data other than the consent requirement for selling consumer health data. If a consumer health data controller meets the applicability thresholds to be subject to the remainder of the law, however, then the law grants individuals:</p> <ul style="list-style-type: none"> <li>• The <b>right to confirm</b> whether a controller is processing the consumer's personal data and to <b>access</b> such data;</li> <li>• The <b>right to correct</b> inaccuracies in their personal data;</li> <li>• The <b>right to obtain a copy</b> of the consumer's personal data processed by the controller in a portable and readily usable format;</li> <li>• The <b>right to revoke consent</b> provided by the consumer (processing must cease "as soon as practicable" and within 15 days);</li> <li>• The <b>right to delete</b> personal data provided by, or obtained about, the consumer;</li> <li>• The <b>right to opt out</b> of the processing of the personal data for purposes of <b>targeted advertising</b>, the <b>sale</b> of personal data, or <b>profiling</b> in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.</li> </ul> <p>Conn. Gen. Stat. § 42-518 (2024).</p>	<p>» <b>New York and Washington are Largely Aligned:</b> The individual rights afforded by New York's and Washington's laws are similar in scope and intent. Both offer rights to access covered data, revoke consent previously given, and delete their covered data. There are some differences in how these rights are exercised, however. Most notably, New York's right to revoke authorization is written to be <b>immediate</b> rather than "as soon as practicable". New York's implicit requirement for the immediate deletion of data pursuant to revoking authorization may be impracticable given how businesses store and backup personal information.</p> <p>» <b>Connecticut Has Limited Health-Specific Rights:</b> Connecticut's rights are both broader and narrower than New York and Washington depending on whether a consumer health data controller is also a controller subject to the full comprehensive privacy law. Entities that are only consumer health data controllers are only required to offer the right to revoke consent. Entities that are subject to the full law must comply with additional rights of access, correction, deletion, portability, and opt-outs.</p>

 <b>Comparison of Consumer Health Privacy Frameworks: New York, Washington, and Connecticut</b>			
New York Health Information Privacy Act	Washington My Health My Data	Connecticut SB 3	FPF Analysis
<b>Individual Rights: Timing</b>			
<p>Regulated entities have <b>30 days</b> to comply with <b>access and deletion</b> requests.</p> <p>For <b>authorization</b>, the regulated entity must provide a mechanism "by which an individual may <b>revoke authorization at any time</b>." Upon revocation, the regulated entity must <b>"immediately cease all processing activities</b> for which authorization was revoked, except to the extent necessary to comply with the regulated entity's legal obligations."</p> <p>§§ 1122(2)(c); 1123(1)-(2).</p>	<p>Regulated entities shall comply with consumer requests <b>"without undue delay"</b> and <b>within 45 days</b> of receipt, which may be extended once by 45 additional days "when reasonably necessary."</p> <p>This 45 day response period applies to the exercise of consumer rights, including revoking consent for processing, but it does not apply to revoking valid authorization.</p> <p>Wash. Rev. Code § 19.373.040.</p>	<p>Controllers must respond to a request <b>"without undue delay"</b> and <b>within 45 days</b>, which may be extended once by an <b>additional 45 days</b> "when reasonably necessary." Conn. Gen. Stat. § 42-518(c) (2024).</p> <p>Controllers must provide an effective mechanism for consumers to revoke consent and, once a consumer revokes consent, must "cease to process the data as soon as practicable, but not later than fifteen days after the receipt of such request."</p> <p>Conn. Gen. Stat. §§ 42-518 &amp; 42-520 (2024).</p>	<p>New York generally requires faster turnaround in complying with rights requests than Washington or Connecticut.</p> <p>» <b>Shorter Deadline; No Extension:</b> New York gives a shorter time frame for complying with access and deletion rights—30 days versus 45—and does not allow for a one-time extension. However, Washington and Connecticut require that rights requests be complied with "without undue delay," which could require faster compliance with rights requests than New York.</p> <p>» <b>Revoking Authorization is Immediate:</b> Additionally, under New York when an individual revokes authorization, a company must "immediately cease all processing activities," which could be interpreted as an instant deletion requirement.</p>
<b>Exercising &amp; Verifying Rights Requests</b>			
<p>A regulated entity must establish "effective, efficient, and easy-to-use" mechanisms for individuals to revoke authorization, submit an access request, and submit a deletion request.</p> <p>§§ 1122(2)(c); 1123(1)(a); 1123(2)(a).</p>	<p>Consumers can exercise their rights by submitting a request which may be made by a "secure and reliable means established by the regulated entity" and which "must take into account the ways in which consumers normally interact with the regulated entity" and regulated entity's ability to "authenticate the identity of the consumer making the request."</p> <p><b>Verification:</b> A regulated entity is not required to comply with a request if it is not able to, <b>using commercially reasonable efforts</b>, authenticate the request, and it may request that the consumer "provide additional information <b>reasonably necessary to authenticate</b> the consumer and the consumer's request."</p> <p>Wash. Rev. Code § 19.373.040.</p>	<p><b>Note:</b> This applies only if a consumer health data controller is also a <b>controller</b> and therefore subject to the broader obligations and individual rights under the law that apply to processing personal data</p> <p>Consumers can exercise their rights by submitting a request to a controller by a "secure and reliable means established by the controller and described" in its privacy notice. Consumers can exercise some opt-out rights via an authorized agent or an opt-out preference signal.</p> <p><b>Verification:</b> A controller is not required to comply with a request if it is not able to, <b>using commercially reasonable efforts</b>, authenticate the request, and it may request that the consumer "additional information reasonably necessary to authenticate such consumer and such consumer's request." Controllers are not required to authenticate opt-out requests but may deny an opt-out request if it has a "good faith, reasonable and documented belief that such request is fraudulent," in which case it must notify the requester. Controllers must also establish a process for consumers to appeal the controller's refusal to act on a request.</p>	<p>» <b>No Flexibility to Deny Unverified Consumer Requests:</b> New York is the only framework that includes no provisions requiring regulated entities to verify the identity of individuals submitting rights requests. This could have significant negative impacts for consumers if it enables bad actors to submit fraudulent access and deletion requests.</p> <p>A regulated entity could make the argument that a mechanism for exercising individual rights cannot be "effective" as required under the Act if it does not account for commercially reasonable verification. Similarly, not verifying requests would be at odds with the requirement to "develop, implement, and maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of regulated health information."</p>
<b>Regulated Entity Duties</b>			
<p>New York establishes the following duties for regulated entities:</p> <ul style="list-style-type: none"> <li>Must provide <b>notice</b> to individuals about the types of RHI processed, the nature and specific purposes of its processing, and other information. § 1122(3)(a).</li> <li>To "develop, implement, and maintain <b>reasonable administrative, technical, and physical safeguards</b> to protect the security, confidentiality, and integrity of [RHI]." § 1124(1).</li> <li><b>Non-retaliation.</b> § 1122(2)(g).</li> <li><b>Disposal</b> of an individual's RHI pursuant to a <b>publicly available retention schedule</b> within a reasonable time (and no later than 60 days) once "it is no longer necessary to maintain" for the purposes for which it was collected. § 1124(2).</li> </ul>	<p>Regulated entities must:</p> <ul style="list-style-type: none"> <li>Maintain and adhere to a <b>"consumer health data privacy policy"</b> that makes a specific set of disclosures and to "prominently publish" a link to this policy on its homepage;</li> <li><b>Restrict access</b> to consumer health data to necessary employees, processors, and contractors;</li> <li>Establish, implement, and maintain <b>reasonable data security practices</b>;</li> <li>Establish a <b>consumer appeals process</b>; and</li> <li>Not <b>"unlawfully discriminate"</b> against a consumer for exercising their rights.</li> </ul> <p>Wash. Rev. Code §§ 19.373.020–19.373.050, 19.373.080.</p>	<p>Regulated entities are <b>prohibited</b> from:</p> <ul style="list-style-type: none"> <li>Providing <b>employees or contractors with access</b> to consumer health data unless they are subject to a "contractual or statutory <b>duty of confidentiality</b>"; or</li> <li>Providing processors with access to consumer health data unless both parties comply with section 42-521 [processors' duties &amp; contractual obligations].</li> </ul> <p>Conn. Gen. Stat. § 42-526 (2024).</p>	<p>» <b>Fewer Duties, but Novel Retention Limit:</b> While New York omits some of the duties in MHMD, such as establishing a consumer appeals process, New York's requirement for a publicly available retention schedule is unique and goes beyond MHMD as well as many other privacy laws. Connecticut imposes a broader array of obligations for entities that are subject to the entire privacy act, but its duties specific to consumer health data align with Washington and New York.</p> <p>Prohibitions on geofencing are not included in this chart.</p>

<div>  <div> <div>Comparison of Consumer Health Privacy Frameworks:</div> <div>New York, Washington, and Connecticut</div> </div> </div>			
New York Health Information Privacy Act	Washington My Health My Data	Connecticut SB 3	FPF Analysis
Processor Duties			
<p>Processing must be governed by a "written, binding agreement" that sets forth clear instructions for processing. § 1125. The bill details a number of requirements that must be in the agreement, including that service providers must:</p> <ul style="list-style-type: none"> <li>• Have a <b>duty of confidentiality</b>;</li> <li>• Protect RHI in a manner consistent with the act;</li> <li>• Only process data <b>to the extent necessary to comply with its obligations</b> to the regulated entity;</li> <li>• <b>Cannot</b> combine the RHI it receives with other personal information it has about individuals;</li> <li>• <b>"Comply"</b> with exercise of an individual's rights upon the request of regulated entities;</li> <li>• Must cooperate with <b>"reasonable assessments"</b> by the regulated entity or the entity's assessor for purposes of evaluating compliance.</li> </ul>	<p>Processors must:</p> <ul style="list-style-type: none"> <li>• Only process consumer health data contract between the processor and the regulated entity; and</li> <li>• Assist regulated entities in fulfilling their obligations under the Act.</li> </ul> <p>Processors that do not follow a regulated entity's instructions or process consumer health data outside the scope of their contract with a regulated entity are <b>"considered a regulated entity"</b> . . . with regard to such data."</p> <p>Wash. Rev. Code § 19.373.060.</p>	<p>Processors must:</p> <ul style="list-style-type: none"> <li>• Adhere to the controller's instructions and assist the controller in meeting the controller's obligations under the Act;</li> <li>• Only process consumer health data pursuant to a binding contract with the controller that, among other things, imposes a duty of confidentiality with respect to the data.</li> </ul> <p>Processors who do not follow a controller's instructions or begins to determine the "purpose and means" of processing personal data is a controller and not a processor with respect to such processing.</p> <p>Conn. Gen. Stat. §§ 42-521 &amp; 42-526 (2024).</p>	<p>» <b>Heightened Processor Duties:</b> New York provides a more detailed and prescriptive list of processor obligations than Washington, specifying what must be included within a contract between the service provider and the regulated entity.</p>
Enforcement			
<p>New York provides for <b>enforcement by the New York Attorney General</b>. § 1127(1).</p> <ul style="list-style-type: none"> <li>• The NY AG's office may enjoin any violation and may seek restitution, disgorgement of profits directly or indirectly obtained, civil penalties of up to \$15,000 per violation or 20% of revenue obtained from NY consumers in the past year, whichever is greater.</li> </ul> <p>New York states that the remedies provided by this section shall be in addition to any other lawful remedy available. § 1127(2).</p>	<p>Violations of the Act are <b>unfair or deceptive acts in trade or commerce</b> under the Washington Consumer Protection Act (WCPA). The WCPA provides for enforcement by the <b>Washington Attorney General</b> (WA AG) as well as through a <b>private right of action</b>.</p> <ul style="list-style-type: none"> <li>• The WA AG's office may seek injunctive relief as well as monetary damages for restitution and legal costs, including reasonable attorney's fees.</li> <li>• Upon showing injury to business or property, individuals may seek injunctions and actual damages (including legal fees). The court has discretion to award treble damages up to \$25,000.</li> </ul> <p>Wash. Rev. Code §§ 19.373.090, 19.86.080 &amp; 19.86.090.</p>	<p>Violations are enforced <b>solely and exclusively</b> by the Attorney General (AG) as violations of Connecticut's prohibition on unfair trade practices. The law explicitly provides that nothing in the Act "shall be construed as providing the basis for, or be subject to, a private right of action for violations of said sections or any other law." The AG has discretion as to whether to allow a controller a right to cure violations.</p> <p>Conn. Gen. Stat. § 42-525 (2024).</p>	<p>» <b>Private Right of Action Ambiguity:</b> Washington explicitly provides for a private right of action whereas Connecticut explicitly provides that no cause of action exists under the law or under any other law. New York, in contrast, does not explicitly provide for a private right of action but may open the possibility of certain "backdoor" claims by declining to provide for "exclusive" AG enforcement.</p>

This is a work product of FPF's U.S. Legislation team, drafted by Jordan Francis (Policy Counsel), Bailey Sanchez (Deputy Director) & Keir Lamont (Senior Director)

**Note:** This chart was created using the version of the New York Health Information Privacy Act as it passed the legislature on January 22, 2025. This chart is for informational purposes only and should not be used as legal advice.