PENALTIES FOR INAPPROPRIATE DISCLOSURES OR USES OF DIRECT AND INDIRECT PATIENT IDENTIFIERS AND PROPRIETARY FINANCIAL INFORMATION

A. INTRODUCTION

Chapter 43.371 RCW contains provisions that direct the Office of Financial Management (OFM) to establish and adopt rules related to a statewide All Payer Claims Database (WA-APCD). Paper 7 provides background information for the rule required in RCW 43.371.070(1)(h) — penalties for the inappropriate disclosures or uses of direct patient identifiers, indirect patient identifiers and proprietary financial information.

Chapter 43.371 RCW defines the following terms related to the rule:

- "Direct patient identifier" means a data variable that directly identifies an individual, including names; telephone numbers; fax numbers; Social Security number; medical record numbers; health plan beneficiary numbers; account numbers; certificate or license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; web universal resource locators; internet protocol address numbers; biometric identifiers, including finger- and voice prints; and full face photographic images and any comparable images. (See RCW 43.371.010(7).)
- "Indirect patient identifier" means a data variable that may identify an individual when combined with other information. (See RCW 43.371.010(9).)
- "Proprietary financial information" means claims data or reports that disclose or would allow the determination of specific terms of contracts, discounts or fixed reimbursement arrangements or other specific reimbursement arrangements between an individual health care facility or health care provider, as those terms are defined in RCW 48.43.005, and a specific payer or internal fee schedule or other internal pricing mechanism of integrated delivery systems owned by a carrier. (See RCW 43.371.010(12).)

Chapter 43.371 RCW does not define "disclosure" nor is this term defined in other Washington state statutes. However, the federal 1996 Health Insurance Portability and Accountability Act — one of the key federal laws for the privacy and security of health information — defines "disclosure." "Disclosure" means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.[1]

Chapter 43.371 RCW is silent on what constitutes "inappropriate uses" thereby leaving the discussion to the rule-making process.

On April 23, 2015, the OFM director received the letter in Exhibit A clarifying the legislative intent of this rule.

1. For the definition of disclosure, see http://www.hipaa.com/the-definition-of-disclosure/.

EXHIBIT A

RECEIVED

APR 23 2015

OFM DIRECTOR'S OFFICE

April 17, 2015

Washington State Legislature

David Schumacher
Director
Office of Financial Management

Dear Mr. Schumacher,

The Legislature recently passed ESSB 5084, a bill modifying the laws governing Washington's All Payer Claims Database. This bill is the result of extensive attention and work by members of the House and Senate, stakeholders, and staff. It was carefully and deliberately tailored to balance appropriate access and use of claims and financial data, with appropriate security measures and constraints.

Protecting the confidentiality and security of patient information was paramount throughout the process and in the final product.

We are writing to clarify our intent regarding a specific section in ESSB 5084. Section 7 of the final bill directs the Office of Financial Management to adopt rules to establish the penalties associated with the inappropriate disclosures or uses of direct patient identifiers, indirect patient identifiers, and proprietary financial information. Although we did not specify further detail in the bill, **it is our desire and expectation that the rulemaking consider setting penalties at the highest level possible** to discourage any inappropriate uses of confidential claims and financial data.

We know you will share our desire to protect this sensitive data and thank you for your consideration.

Please pass along our appreciation to your staff for all the assistance they provided during the development and refinement of this bill. We are interested in tracking the development of the rules and the full implementation of the database, and stand ready to assist you and your staff as needed.

Sincerely,

Randi W Becker

Senator Randi Becker
Chair, Senate Health Care Committee

Eileen Cody

Representative Eileen Cody
Chair, House Health Care and Wellness

To develop effective WA-APCD penalties that meet legislative intent, OFM reviewed examples of civil and criminal penalties related to inappropriate disclosures or uses of personal health care information. OFM also reviewed penalties in relevant federal and Washington state statutes, and in other state APCD rules, as well as data use agreements and confidentiality agreements. OFM also examined penalties for data breaches in 47 states, some of which do not have APCDs. The statutes that OFM reviewed are:

- The 1996 Health Insurance Portability and Accountability Act (HIPAA). HIPAA is a federal law enacted to provide a variety of protections for individuals and their health insurance, including access, portability, fraud and abuse protections and administrative simplification. HIPAA laid the groundwork for the privacy and security of health information. It includes penalty provisions for noncompliance.
- The 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act. HITECH is a federal law enacted as part of the American Recovery and Reinvestment Act to promote the adoption of health information technology. HITECH enhanced the enforcement of HIPAA with more stringent penalty provisions.2
- The following Washington state statutes:
  - Chapter 42.48 RCW Release of Records for Research
  - Chapter 70.02 RCW Medical Records–Health care information access and disclosure
  - Chapter 74.04 RCW Public Assistance General Provisions–Administration
  - RCW 19.255.010 Disclosure notice–Definitions–Right and remedies
  - RCW 42.56.590 Personal information–Notice of security breaches

Paper 7 is divided into the following sections:

B. WHAT ARE CIVIL AND CRIMINAL PENALTIES?

A penalty is a punishment imposed by statute as a consequence of the commission of a certain specified offense. A penalty includes both *fines* and *forfeiture.* A *fine* is a pecuniary penalty. A *forfeiture* is a penalty by which one loses rights and interest in one's property.[3]

2. In February 2013, the omnibus rule to incorporate the statutory provisions of HITECH in HIPAA was adopted with an effective date of September 2013.
3. Definition of "penalty" from Black's Law Dictionary.

Penalties are divided into two categories: *civil* (noncriminal) and *criminal*. Civil penalties are fines or surcharges imposed by government agencies to enforce laws and regulations, such as late payment of taxes, failure to obtain a permit, etc. The penalty for failure to file claims as required for the WA-APCD is classified as a civil penalty and imposed by a government agency.[4]

Civil penalties can be quite significant and result in the penalty recipient losing rights and property, such as losing a license or registration to do business in a state. Before imposing a penalty, the government agency must ensure that the subject of the penalty is afforded due process of law.[5] Government agencies provide due process by following an administrative process.

In Washington state, the civil penalties that are pecuniary are structured in a variety of ways, including:

- A fixed dollar amount.
- Maximum and minimum dollar amounts.
- A schedule of escalating penalties to address additional or more severe violations.
- A percentage of remittance due plus interest (usually used for late tax payments).

Funds collected from penalties are deposited in the state General Fund unless otherwise specified in statute.

Before imposing penalties, Washington state agencies follow an administrative process to provide due process set forth in the Administrative Procedures Act, Chapter 34.05 RCW. Steps taken prior to imposing a penalty may include the following:

- Provide a warning notice outlining the violation(s) and the possible penalties.
- Allow a time period for the subject to correct the violation(s).
- Provide an opportunity for the subject to respond to the penalty, including an opportunity to present extenuating circumstances that prevent compliance.
- Allow a penalty waiver or extension for payment for extenuating circumstances.

As alluded to above, Washington state agencies may allow for extenuating circumstances to mitigate the penalty imposed. Some agencies also allow for good behavior to mitigate the penalty. For example, if a previously penalized entity is compliant for a period of time, the state agency may waive the penalty on the next occurrence of noncompliance.

Criminal penalties are imposed for felonies and misdemeanors.[6] Felonies are the most serious crimes, such as rape, armed robbery, burglary, and sales or distribution of illegal drugs, usually punishable by imprisonment for a term exceeding one year. Punishment may also include imposing fines. For the most egregious felonies, some states may impose the death penalty.

---

4. See WAC 82-75-090 under Chapter 82-75 WAC, http://www.ofm.wa.gov/rulemaking/rules_adopted/WSR_16-04-068_OTS-7546_3.pdf.
5. The Fifth and 14th Amendments of the U.S. Constitution state that no one shall be "deprived of life, liberty, or property without due process of law." This is known as the due process clause. Article 1, Section 3 of the Washington State Constitution provides that no person shall be "deprived of life, liberty, or property, without due process of law."
6. See Black's Law Dictionary definitions of felony and misdemeanor: http://www.criminallawfirmseattle.com/Criminal-Defense/Felonies-Misdemeanors.aspx and http://app.leg.wa.gov/RCW/default.aspx?cite=9A.20.

In Washington, the Legislature must authorize in statute the imposition of criminal penalties for violations of a law. RCW 9A.20.010 categorizes felonies into classes A, B or C, in descending order of seriousness. Under RCW 9A.20.021, the maximum sentences for felonies are:

- Class A felonies: a fine of up to $50,000, or both a fine and imprisonment. Class A felonies are the most serious and can result in penalties of up to life in prison.
- Class B felonies: up to 10 years in prison, a fine of up to $20,000, or both a fine and imprisonment.
- Class C felonies: up to 5 years in prison, a fine of up to $10,000, or both a fine and imprisonment.

In Washington, felony cases are heard in superior court. Some felonies have a statute of limitations, which is the time period within which a legal proceeding must be commenced. If the state fails to bring a case within the specified time period, it loses its right to prosecute for that crime forever.[7]

Misdemeanors are offenses that are less serious than felonies and generally punishable by fine or imprisonment in a penitentiary or a county jail, depending on the length of imprisonment. Under federal law and most state laws, any offense other than a felony is classified as a misdemeanor.

In Washington state, misdemeanors are often regarded as minor criminal offenses and divided into misdemeanors and gross misdemeanors. Examples of misdemeanors are shoplifting and disorderly conduct. A gross misdemeanor is a more serious offense. For instance, driving while under the influence of alcohol and/or drugs as a first offense is an example of a gross misdemeanor. Under RCW 9A.20.021, the maximum sentences that can be fixed by the court are:

- Misdemeanor: imprisonment in the county jail for a maximum term of not more than 90 days, or a fine of not more than $1,000, or by both imprisonment and a fine.
- Gross misdemeanor: imprisonment in the county jail for not more than 364 days, or a fine of not more than $5,000, or by both imprisonment and a fine.

Penalties often depend on the nature of the offense, any aggravating factors involved and the criminal history of the offender.

In Washington, misdemeanor cases are heard in district and municipal courts. The statute of limitations to prosecute a misdemeanor is one year after its commission. The statute of limitations to prosecute a gross misdemeanor is two years after its commission.

C. CIVIL AND CRIMINAL PENALTIES UNDER HIPAA AND HITECH

Violations of HIPAA can result in both civil and criminal penalties. Under HIPAA, the maximum civil penalty that could be imposed for a HIPAA violation was $100 per violation, with a total amount of $25,000 for all violations of an identical requirement or prohibition during a calendar year. Only covered entities were subject to penalties.[8]

7. See RCW 9A.04.070 Limitations of actions http://app.leg.wa.gov/rcw/default.aspx?cite=9A.04.080/.
8. Covered entities are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses and (3) health care providers who electronically transmit any health information in connection with transactions for which the U.S. Department of Health and Human Service has adopted standards. See http://www.hhs.gov/hipaa/for-professionals/covered-entities/.

The HITECH Act established a much more stringent civil and criminal penalty structure for HIPAA violations and extended the liability for violations to business associates.[9] The civil penalty structure is:

- Four categories of violations that reflect increasing levels of culpability.[10]
- Four corresponding tiers of civil penalty amounts that significantly increase the minimum penalty amount for each violation.
- A maximum penalty amount of $1.5 million per calendar year for violations of an identical provision.

The levels of culpability are:

- *Did not know*. The covered entity or business associate did not know and by exercising reasonable diligence, would not have known that the covered entity or business violated a provision.
- *Reasonable cause*. Violation in which it is established that the violation was due to reasonable cause and not to willful neglect.[11]
- *Willful neglect — corrected*. For a violation in which it is established that the violation was due to willful neglect and was corrected within 30 days of discovery.[12]
- *Willful neglect — uncorrected*. For a violation in which it is established that the violation was due to willful neglect and was not corrected within 30 days of discovery.

Table 1 lists the civil penalty amounts for each level of culpability and the calendar year cap for violations of an identical provision.[13]

Table 1: Categories of violations and civil penalty amounts

Violation category	Civil penalty for each violation	Total civil penalty per year (for all violations of an identical provision)
Did not know	$100 – $50,000	$1,500,000
Reasonable cause	$1,000 – $50,000	$1,500,000
Willful neglect –- corrected	$10,000 – $50,000	$1,500,000
Willful neglect – not corrected	$50,000	$1,500,000

Source: Federal Register /Vol. 78, No. 17 / Friday, January 25, 2013 /Rules and Regulations page 5583. See https://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf?utm_source=buffer&utm_campaign=Buffer&utm_content=buffer5bc4f&utm_medium=twitter.

9. A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. See http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/.

10. Black's Law Dictionary defines "culpability" as blameworthiness. A person's criminal culpability requires a showing that he acted purposely, knowingly, recklessly or negligently, as the law may require, with respect to each material element of the offense.

11. "*Reasonable cause* means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect." 45 CFR 160.401, at 78 *Federal Register* 5691

12. Black's Law Dictionary defines "willful neglect" as the intentional disregard of a plain or manifest duty, in the performance of which the public or person injured has an interest.

13. Civil monetary penalties are not the exclusive remedy for HIPAA violations. The U.S. Department of Health and Human Services Office of Civil Rights has discretion to use other measures to address HIPAA violations, such as providing direct technical assistance or resolving possible noncompliance through informal means.

The U.S. Department of Health and Human Services Office of Civil Rights (OCR) is responsible for investigating alleged HIPAA violations. OCR determines the nature and extent of the violations, the nature and extent of the resulting harm and the total number of violations. To determine the penalty amount, OCR considers the following factors:

- The nature and extent of the violation, including but not limited to the number of individuals affected and the time period during which the violation occurred.
- The nature and extent of the harm resulting from the violation, including but not limited to:
  - Whether the violation caused physical harm.
  - Whether the violation resulted in financial harm.
  - Whether the violation resulted in harm to an individual's reputation.
  - Whether the violation hindered an individual's ability to obtain health care.
- The history of compliance with the administrative simplification provisions, including violations, by the covered entity or business associate, including but not limited to:
  - Whether the current violation is the same or similar to previous indications of noncompliance.
  - Whether and to what extent the covered entity or business associate has attempted to correct previous indications of noncompliance.
  - How the covered entity or business associate has responded to technical assistance provided in the context of a compliance effort.
  - How the covered entity or business associate has responded to prior complaints.
- The financial condition of the covered entity or business associate, including but not limited to:
  - Whether the covered entity or business associate had financial difficulties that affected its ability to comply.
  - Whether the imposition of a civil money penalty would jeopardize the ability of the covered entity or business associate to continue to provide or to pay for health care.
  - The size of the covered entity or business associate.
  - Other relevant considerations.

In the case of a continuing violation of a provision, a separate violation occurs each day the covered entity or business associate is in violation of the provision. OCR does not impose the maximum penalty amount in all cases but rather determines the amount of the penalty on a case-by-case basis.

If a covered entity or business associate is assessed HIPAA penalties, there are several options:

- *Establish an affirmative defense.* This means that the covered entity or business associate corrects the violation within 30 days from the date that the organization had knowledge of the violation or with the exercise of reasonable diligence would have had knowledge of the violation or during a period determined appropriate by OCR.
- *Ask the penalty be waived.* Under the rules, OCR has the discretion to waive a civil penalty amount (CMP) for violations that are not due to willful neglect in whole or in part to the extent that the penalty is excessive relative to the violation. The waiver power mirrors the tiered CMP structure by providing a mechanism to ensure that the amount of CMP reflects the level of culpability.
- *Appeal the penalty.*

The criminal penalties for HIPAA violations include monetary fines or imprisonment or both. The criminal penalty structure is divided into: [14]

- Three categories of violations reflecting increasing levels of culpability.
- Three corresponding tiers of monetary penalty amounts that significantly increase the minimum penalty amount for each violation.
- Three corresponding tiers for imprisonment length.

The categories of violations and levels of culpability are:

- If a person knowingly and in violation of wrongful disclosure of individually identifiable health information (IIHI):[15]
  - Uses or causes to be used a unique health identifier;
  - Obtains IIHI relating to an individual; and
  - Discloses IIHI to another person.
- If the crime was committed under false pretenses.
- If an offense is committed with intent to sell, transfer or use IIHI for commercial advantage.

For each category of violation there are three possible penalties:

- A fine only
- Imprisonment only
- Or both a fine and imprisonment

Table 2 lists the maximum monetary penalty amount and prison sentence for each violation category.

Table 2: Categories of violations and respective criminal penalties

Violation category	Monetary penalty only	Imprisonment term only	Monetary penalty and imprisonment
Knowingly and wrongfully discloses IIHI	Not more than $50,000	Not more than 1 year	Not more than $50,000 and not more than 1 year in prison
Under false pretenses	Not more than $100,000	Not more than 5 years	Not more than $100,000 and not more than 5 years in prison
Intent to sell, transfer or use for commercial advantage	Not more than $250,000	Not more than 10 years	Not more than $250,000 and not more than 10 years in prison

Source: https://www.healthlawyers.org/hlresources/Health%20Law%20Wiki/HITECH%20Act.aspx

Penalties are imposed based on the facts of each individual case and if the individual profited from the theft, access or disclosure of IIHI. The judge may determine that it is necessary for all moneys received to be refunded, in addition to the payment of a fine.[16]

14. http://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/
15. Person health information is individually identifiable health information with a few exceptions. See http://www.hipaasurvivalguide.com/hitech-act-business-associates.php.
16. In June 2005, the U.S. Department of Justice concluded that the criminal penalties for a violation of HIPAA are directly applicable to covered entities, including health plans, health care clearinghouses, health care providers who transmit claims in electronic form and Medicare prescription drug card sponsors. Individuals such as directors, employees or officers of the covered entity, where the covered entity is not an individual, may also be directly criminally

Under the HITECH Act, state attorneys general are given authority to prosecute HIPAA violations where there is reason to believe that the interest of one or more state residents has been or is threatened by a HIPAA violation. State attorneys general are limited to the first tier maximums for civil monetary penalties — $100 per violation, with a $25,000 yearly maximum. OCR can impose the higher penalty amounts. Table 3 illustrates the levels of penalties that state attorneys general and OCR can impose.[17]

Table 3: Statutory damages applied by state attorneys general and Office of Civil Rights

For violations	Limits for state attorneys generals for violations against one or more state residents	Statutory damage limits for OCR
Damages/penalty amount	Up to $100 per violation	$100 to $50,000 or more per violation
Calendar year cap	$25,000	$1,500,000

Source: Washington HealthCare News, July 2012

D. CIVIL AND CRIMINAL PENALTIES IN OTHER STATE APCD LAWS AND RULES

Maine and Vermont have penalties in rules. Colorado, Massachusetts and Maryland have penalties in their data use agreements (DUA) and confidentiality agreements.

Maine

The APCD administrator — the Maine Health Data Organization (MHDO) — is authorized in rule to impose fines for violations of the laws and rules for safeguarding individual patient identification and confidential information. These fines are in addition to other applicable civil and criminal penalties that may be imposed for a violation.

A fine of not more than $500,000 may be imposed for intentional or knowing use, sale or transfer of the APCD data in violation of the board's rules for commercial advantage, pecuniary gain,[18] personal gain or malicious harm.[19] The fine may be imposed against any person or entity that receives data or information under the data release process or who has access to APCD data, such as an MHDO employee or vendor.

liable under HIPAA in accordance with principles of corporate criminal liability. Where individuals of a covered entity are not directly liable under HIPAA, they can still be charged with conspiracy or aiding and abetting. The department interpreted the "knowingly" element of the HIPAA statute for criminal liability as requiring only knowledge of the actions that constitute an offense. Specific knowledge of an action being in violation of the HIPAA statute is not required. See http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page.

17. See "HIPAA Civil Monetary Penalties: Is there a limit?" by Emily R Studebaker and Stephen D. Rose, Washington Healthcare News, July 2012 http://www.wahcnews.com/newsletters/Volume7Issue7WAHealthcareNews.pdf.

18. Pecuniary gain refers to a gain of monetary value. In criminal law, the term refers to any monetary or economic gain that serves as an impetus for the commission of an offense. See http://definitions.uslegal.com/p/pecuniary-gain/.

19. Malicious intent refers to the intent, without just cause or reason, to commit a wrongful act that will result in harm to another. It is the intent to harm or some evil purpose. See http://definitions.uslegal.com/m/malicious-intent/.

A fine of up to $2,500 may be imposed on a person[20] or entity[21] that:

- Violates a provision of the data use agreement.
- Does not return or destroy APCD data when directed to by the executive director.
- Does not modify a document that contains or uses APCD data in accordance with the directives of the MHDO executive director.

Each day that the violation exists may be considered a separate occurrence.

The following factors are considered before imposing a fine:

- The amount of the data misused.
- Whether the misused data involved any personal health information (PHI).
- Amount of any gain involved.
- Extent of harm to the individual whose data was misused.
- Any other criteria deemed pertinent to such a fine.

A person or entity that is penalized may petition the MHDO board for review of the decision. The petition must be filed within 15 business days. If the MHDO board denies the petition in whole or in part, the person or entity can appeal to the superior court.

If the person or entity that was penalized fails to pay the fine levied, the MHDO board may take further legal action in superior court.

Vermont

In Vermont, the commissioner is authorized in rule to impose an administrative penalty on any person who knowingly:

- Fails to comply with confidentiality requirements.
- Uses, sells or transfers the data or information for commercial advantage, pecuniary gain, personal gain or malicious harm.

The penalty is not more than $50,000 per violation and is in addition to any other penalties, fines or forfeitures authorized by law.[22]

Penalties for violations of data use agreements

In other states, violations of APCD data use agreements constitute misuse and can result in the imposition of nonmonetary, civil and/or criminal penalties against the data recipient(s). OFM reviewed the penalties included in the DUAs in Colorado, Massachusetts, Maryland, New Hampshire and Oregon.

20. In 90-590 MHDO Chapter 100 Enforcement Procedures, "person" means an individual, trust, estate, partnership, corporation including associations, joint stock companies and insurance companies, the state or any political subdivision or instrumentality, including a municipal corporation of the state, or any other legal entity recognized by state law.
21. In 90-590 MHDO Chapter 100 Enforcement Procedures, "entity" means an assessed, commercial, educational or nonprofit entity as defined by the MHDO Prices for Data Sets, Fees for Programming and Report Generation and Duplication Rates Rule (90-590 C.M.R. Chapter 50).
22. See Regulation H-2008-01Vermont Healthcare Claims Uniform Reporting and Evaluation System at http://www.dfr.vermont.gov/sites/default/files/REG-H-08-01.pdf.

Colorado

In Colorado, violations of the terms of the DUA constitute a breach of contract. This may result in nonmonetary, civil and criminal penalties. The nonmonetary penalties are:

- The immediate surrender and return of all APCD data.
- Denial of future access to APCD data.

Civil and criminal penalties may result from:

- Civil action by the administrator for breach of contract.
- A complaint filed with OCR that may result in civil and criminal penalties.
- The Colorado state attorney general acting under the authority granted to the state attorneys general under the HITECH Act to take civil action on certain HIPAA violations.

Massachusetts

In Massachusetts, violations of the terms of the DUA may result in liabilities or penalties under federal law, the Massachusetts privacy law[23] and law on the regulation of business practices for consumer protection.[24]

Maryland

In Maryland, breach of a DUA may result in:

- Conducting an investigation, including an onsite investigation.
- Resolving the dispute by a correction plan.
- Declaring of a breach and demanding return of the data.
- Providing no further data.

Other remedies to resolve a DUA breach include pursuing all legal, equitable and criminal remedies. In the event that the Maryland Health Care Commission is successful in a court action, the data requester has to pay reasonable attorney's fees and costs to the commission.

New Hampshire

In New Hampshire, failure to adhere to the terms of the DUA results in the immediate recall of all data sets. The data recipient is also prohibited from using, disclosing or publishing any report, publication or presentation derived from the data sets.

Oregon

In Oregon, failure to comply with the terms of the DUA for public use data sets is grounds for immediate termination of the agreement. Wrongful use or disclosure of information may result in:

- Immediate revocation of access to the data.
- An opportunity to correct the unauthorized use or disclosure and end the violation. Access is terminated if investigators do not cure the unauthorized use or disclosure.

[23] See Massachusetts General Laws Chapter 214 Section 1B https://malegislature.gov/Laws/GeneralLaws/PartIII/TitleI/Chapter214/Section1.
[24] See Massachusetts General Laws, Chapter 93A, Section 4 Actions by attorney general; notice; venue; injunctions https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93A/Section.

Other states: DUA violations

DUA violations in other states include:

- Disclosing or using data outside the provisions in the DUA.
- Not adhering to the APCD's cell suppression policy.
- Identifying individuals in the APCD data by linking records in the APCD to other individually identifiable sources of data without authorization by the APCD administrator.
- Attempting to ascertain any information removed from or encrypted in the data sets.
- Not providing a copy of results or reports derived from APCD data and information when required to do so by the DUA.
- Reusing or further disclosing the original or derivative data file(s) without prior written approval from the APCD administrator.
- Using, reusing, disclosing, marketing, releasing, showing, selling, renting, leasing, loaning or granting access to data files outside except as permitted by DUA.
- Releasing, furnishing, disclosing, publishing or otherwise disseminating this data to any person.
- Copying data and keeping more than one copy.
- Not destroying all other copies of data.
- Not certifying that data has been destroyed by submitting a written notice to the APCD administrator.
- Not returning data to the APCD administrator at the conclusion of the research.
- Linking to other databases to identify individuals.
- Taking legal, administrative or other actions against individuals, or contacting or assisting others to contact any patients and/or physicians who may be indirectly identified.
- Not providing the APCD administrator with a copy of the report or manuscript or URL at least 20 days prior to releasing any manuscript, report or website URL intended for public dissemination.
- Not modifying the report prior to its release to protect against identification of individuals.
- Attempting to re-identify any individuals from records in the data set or attempt to contact subjects represented in the data.
- Linking with individually identifiable data from any other source.
- Retransferring or re-disseminating in a format that could possibly lead to the identification of an individual.

E. EXAMPLES OF CIVIL AND CRIMINAL PENALTIES IN WASHINGTON STATE LAWS

The following Washington statutes provide examples of civil and criminal penalties for unauthorized disclosures of personal information:

- Chapter 42.48 RCW–Release of records for research allows specific state agencies — the Department of Social and Health Services, Department of Corrections, institutions of higher education[25], Department of Health and Department of Early Learning — to access individually identifiable personal records[26] for research purposes. One of the requirements to access the

25. RCW 28B.10.016 defines "institutions of higher education" as "the state universities, the regional universities, The Evergreen State College, the community colleges, and the technical colleges."
26. In RCW 42.48.010–Definitions, "individually identifiable" means that a record contains information which reveals or can likely be associated with the identity of the person or persons to whom the record pertains. "Personal record" means any information obtained or maintained by a state agency which refers to a person and which is declared exempt from public disclosure, confidential or privileged under state or federal law.

data is that the state agencies have a written and legally binding confidentiality agreement prior to disclosure of the data.[27] RCW 42.48.050 authorizes civil and criminal penalties if there are unauthorized disclosures and violations of any provision of the chapter. The penalties are:

- A gross misdemeanor for an unauthorized disclosure, whether willful or negligent by a research professional who has obtained individually identifiable personal record or record information from a state agency. In Washington, a gross misdemeanor is punishable by imprisonment in the county jail for a maximum term fixed by the court of not more than 364 days, or a fine in an amount fixed by the court of not more than $5,000, or by both imprisonment and a fine.
- A civil penalty of not more than $10,000 for each violation of any provision of the chapter by the research professional or the state agency.

- Title 70 RCW contains provisions for public health and safety. In particular, RCW 70.02.330 penalizes any person who requests or obtains confidential information and records related to mental health services under false pretenses. The penalty is a gross misdemeanor.
- Title 74 RCW contains provisions for public assistance. In particular, RCW 74.04.060 provides for the confidentiality of public assistance records except for purposes directly connected with the administration of Medicaid. RCW 74.04.060(4) states that it is "unlawful, except as provided in this section, for any person, body, association, firm, corporation or other agency to solicit, publish, disclose, receive, make use of, or to authorize, knowingly permit, participate in or acquiesce in the use of any lists or names for commercial or political purposes of any nature. The violation of this section shall be a gross misdemeanor."

F. EXAMPLES OF CIVIL AND CRIMINAL PENALTIES FOR A SECURITY BREACH OF PERSONAL INFORMATION

Forty-seven states, including Washington, have enacted legislation requiring private, governmental or educational entities to notify individuals of security breaches involving personally identifiable information.[28]

The state laws for breach of security have provisions on:

- Who must comply with the law.
- Definition of personal information.[29]
- What constitutes a breach, typically an unauthorized acquisition of data.

27. For details of what must be included in the confidentiality agreement, see RCW 42.48.020 (2)(c) http://app.leg.wa.gov/rcw/default.aspx?cite=42.48.020.

28. Each state defines "breach of security." The most common state definition for breach of security is "the unlawful and unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of personal information." See https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/State_Data_Breach_Statute_Form.pdf.

29. Each state has a definition for personal information. The most common state definition for "personal information" is "An individual's first name or first initial and last name plus one or more of the following data elements: (i) Social Security number, (ii) driver's license number or state-issued ID card number, (iii) account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account and generally applies to computerized data that includes personal information. Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state or local government records, or widely distributed media. In addition, Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. See https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/State_Data_Breach_Statute_Form.pdf.

- Requirements for notice of a breach.
- Exemptions. Breach statutes do not usually apply to encrypted information unless the encryption key has been disclosed.
- Penalties for failure to comply with the notification provisions of the statute and other provisions.[30]
- Most states impose civil monetary penalties for failure to notify.[31]
- Some states have criminal penalties. Idaho imposes a criminal penalty on any government employee who intentionally discloses personal information not subject to disclosure that is otherwise allowed by law. The penalty is a misdemeanor punishable by a fine of not more than $2,000, or imprisonment in the county jail for a period of not more than one year, or both.

Michigan imposes a criminal penalty on a person who provides notice of a security breach when a security breach has not occurred, with the intent to defraud. The penalty is a misdemeanor punishable by:

- Imprisonment for not more than 93 days, or a fine of not more than $250 for each violation, or both.
- For a second violation, imprisonment for not more than 93 days, or a fine of not more than $500 for each violation, or both.
- For a third or subsequent violation, imprisonment for not more than 93 days, or a fine of not more than $750 for each violation, or both.

California and New Hampshire have provisions and penalties in their laws for breach of medical information. The California Health and Safety Code, Section 1280.15 directs clinics, health facilities, home health care agencies and hospices to prevent "unlawful or unauthorized access to, and use or disclosure of, patients' medical information." Penalties for violating the California Health and Safety Code, Section 1280.15 are:

- $25,000 per patient whose information was unlawfully or without authorization accessed, used or disclosed, and up to $17,500 per subsequent occurrence. In determining the amount of the penalty, the California Department of Health must consider the entity's history of compliance with this section and related state and federal legislation, the extent to which the entity detected the violations and took corrective actions, and factor's outside the entity's control which may have prevented compliance.
- A penalty of $100 per day for entities that fail to report the incident to the State Department of Health Services or the affected patients within the 15-day time period.
- Total penalties imposed may not exceed $250,000 per reported event.[32]

New Hampshire's Medical Information Unauthorized Disclosure Notification Statute applies to any person, corporation, facility or institution providing health care services.[33] The statute is triggered by

30. See the National Conference of State Legislatures for links to the data breach laws. http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
31. See Appendix A: Examples of Penalties for Security Breach in Other States.
32. See California Health and Safety Code, Chapter 2 Health Facilities, Article 3, Section 1280.15 http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=HSC&sectionNum=1280.15
33. This includes but is not limited to a physician, hospital, office, clinic, health center or other health care facility, dentist, nurse, optometrist, pharmacist, podiatrist, physical therapist or mental health professional, and any officer, employee or agent of such provider acting in the course and scope of employment or agency related to or supportive of health care services.

the unauthorized use or disclosure of protected health information for marketing or fundraising purposes.[34] Health care providers may be liable even if such use is permissible under federal law.

Individuals whose health records were wrongly disclosed may bring a civil action. If successful, special or general damages of not less than $1,000 for each violation, plus costs and reasonable legal fees, can be awarded.

See Appendix A for examples of civil monetary penalties imposed by states for data breaches.

G. WASHINGTON STATE'S BREACH LAWS

In 2005, the Washington Legislature passed two security breach notification laws: Chapter 19.255 RCW, which applies to any person or business, and RCW 42.56.590, which applies to all state and local agencies. These statutes are triggered upon discovery or notification of a breach in the security system.[35]

There are exemptions to the notification requirements:

- A person, business or agency is not required to disclose a technical breach of the security system that does not seem reasonably likely to subject customers to a risk of harm.
- Data that are "secured" are not subject to the data breach notification requirements. "Secured" is defined as encrypted in a manner that meets or exceeds the National Institute of Standards and Technology standard or is otherwise modified so that the personal information is rendered unreadable, unusable or undecipherable by an unauthorized person. (RCW 19.255.010 and RCW 42.56.590)
- A covered entity under HIPAA is considered in compliance with the Washington data breach notification laws with respect to protected health information if it has complied with HITECH, Section 13402. Covered entities must notify the Washington State Attorney General if more than 500 Washington residents are affected as a result of a single breach.

Notice must be given to residents and to the Washington State Attorney General in the most expedient time possible and without unreasonable delay, no more than 45 calendar days after the breach is discovered. A longer period may be required by law enforcement or to determine the scope of the breach and to restore the integrity of the data system.

34. New Hampshire's Medical Information Unauthorized Disclosure Notification Statute incorporates HIPAA's definition of protected medical information. See https://www.hipaa.com/hipaa-protected-health-information-what-does-phi-include/.
"'Marketing' means a communication about a product or service that encourages recipients of the communication to purchase or use the product or service." Health care providers must also provide individuals an opt-out notice before any personally identifiable health information may be used for fundraising purposes. See http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/.
35. RCW 19.255.010 (4) states that "for purposes of this section, 'breach of the security of the system' means unauthorized acquisition of data that compromises the security, confidentiality or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure."

The penalty provisions in the breach laws are:

- A civil action to recover damages. The action is instituted by any customer or individual injured by a violation.
- Enjoin any person or business or agency that violates, proposes to violate or has violated this statute.36
- The rights and remedies available are cumulative to each other and to any other rights and remedies available under the law.

The Washington State Attorney General may bring an action to enforce the law in the name of the state or on behalf of persons residing in the state.

H. CONSIDERATIONS FOR WA-APCD PENALTIES

Before developing WA-APCD penalties for inappropriate disclosures and uses of direct and indirect patient identifiers and proprietary financial information, OFM must consider the following:

- In Washington, criminal penalties cannot be imposed through the rule-making process but must be authorized by the Legislature. Since there are no provisions in Chapter 43.371 RCW for criminal penalties, all WA-APCD penalties will be civil penalties.
- The legislative intent of this rule is to "consider setting penalties at the highest level possible to discourage any inappropriate uses of confidential claims and financial data." With civil penalties, the "highest level possible" can be achieved with monetary and nonmonetary penalties.
- To be effective, careful thought has to be put into the design of the monetary penalties. The design includes the penalty rate, structure, application and enforcement. See Table 4 for design considerations for monetary penalties.
- Nonmonetary penalties can be very effective deterrents and may:
  - Require that the data requester immediately surrender and return all APCD data.
  - Deny the data requester future access to APCD data.
  - Prohibit the data requester from using, disclosing or publishing any report, publication or presentation derived from the data sets.

Without data, many projects cannot continue, and the project funding may be lost. The lost funding may be an indirect monetary penalty of greater magnitude than the direct imposition of a monetary penalty, depending on the amount of funding that was lost.

36. According to Black's Law Dictionary, "enjoin" means to require a person, by writ of injunction, to perform or abstain or desist from some act.

Table 4: Design considerations for penalties for inappropriate disclosures and uses of direct and indirect patient identifiers and proprietary financial information

Consideration	Questions/Issues
Violations	▪ What constitutes inappropriate use? Inappropriate disclosure? ▪ Should there be a list of actions in rule that are considered "inappropriate use"? ▪ Should there be levels of culpability? If so, should they be the same as HIPAA: did not know; reasonable cause; willful neglect — corrected; willful neglect — not corrected ▪ Penalize each violation? ▪ Should penalty be for the length of time that the data recipient should have known of the violation? If so, should penalty be applied by the day or the week? ▪ Should there be an opportunity to correct the violation thereby avoiding the penalty? ▪ How should violations by subcontractors be handled?
Monetary penalties	▪ Should the monetary penalty be a flat dollar amount? ▪ Not to exceed a maximum dollar amount? ▪ Tiered dollar amount? ▪ Is tiered dollar amount tied to the level of culpability?
Nonmonetary penalties	▪ If a data recipient loses access to data for a violation, should the loss of access to data be for a limited period of time? If so, how long? ▪ Should the data recipient be prohibited from using, disclosing or publishing any report, publication or presentation derived from the data sets?
Imposing the penalty	▪ What factors should be considered before imposing the penalty? ▪ What is the administrative process for imposing the penalty?
Penalty waiver	▪ Should there be a provision in rule for a penalty waiver? ▪ What are the extenuating circumstances to waive a penalty? ▪ Should there be a process to apply for a penalty waiver? If so, what should the process be?
Collecting the penalty	▪ Who collects the penalty? ▪ Who follows up if penalty is not paid?
Reporting/evaluating the penalty	▪ Include penalties assessed in report to the Legislature. ▪ Does the penalty deter noncompliance? ▪ Should penalties be published on APCD website?
Appeal	▪ What factors should be considered in a penalty appeal? ▪ Who handles the penalty appeal?

APPENDIX A

Examples of penalties for security breach in other states

State	Penalty/ Private Right of Action
Florida	An entity that violates the provisions for notification of affected individuals or notification to the Florida Department of Legal Affairs is liable for a civil penalty of $1,000 per day, up to 30 days following any violation and $50,000 per 30-day period thereafter, up to a maximum total of $500,000. These penalties apply per breach and not per individual affected by the breach. The violations are to be treated as unfair or deceptive trade practices under Florida law. There is no private right of action.
Idaho	Any agency, individual or commercial entity that intentionally fails to give notice in accordance with section 28-51-105, Idaho Code, will be subject to a fine of not more than $25,000 per breach of the security of the system. Any governmental employee who intentionally discloses personal information not subject to disclosure otherwise allowed by law is guilty of a misdemeanor and, upon conviction thereof, will be punished by a fine of not more than $2,000, or by imprisonment in the county jail for a period of not more than one year, or both.
Iowa	Violations are an unlawful practice under Iowa's Consumer Fraud Statute. Consequences include damages for injury and a fine of up to $40,000 per violation.
Michigan	A person who knowingly fails to provide any notice of a security breach may be ordered to pay a civil fine of not more than $250 for each failure to provide notice. The aggregate liability for civil fines for multiple violations will not exceed $750,000. The attorney general or a prosecuting attorney may bring an action to recover a civil fine. A person who provides notice of a security breach when a security breach has not occurred with the intent to defraud is guilty of a misdemeanor punishable as follows: (a) Except as otherwise provided under subdivisions (b) and (c), by imprisonment for not more than 93 days or a fine of not more than $250 for each violation, or both. (b) For a second violation, by imprisonment for not more than 93 days, or a fine of not more than $500 for each violation, or both. (c) For a third or subsequent violation, by imprisonment for not more than 93 days, or a fine of not more than $750 for each violation, or both.
Ohio	The attorney general may investigate any violations of these sections and bring an action to collect a civil penalty against a person or agency for failing to comply with the statute. The attorney general can seek a temporary restraining order, preliminary or permanent injunction, and civil penalties if it appears that a person or agency has failed or is failing to comply with §§ 1347.12 and 1349.19 of the Revised Code. Upon finding that a person or agency has failed to comply with the statute, the court will impose a civil penalty as follows: (a) $1,000 for each day the agency or person has intentionally or recklessly failed to comply with the applicable section up to 60 days.

State	Penalty/ Private Right of Action
	(b) $5,000 for each day after 60 days and up to 90 days that the agency or person has intentionally or recklessly failed to comply with the applicable section. (c) $10,000 for each day after 90 days that the agency or person has intentionally or recklessly failed to comply with the applicable section.
Oregon	Compensation can be ordered by the state upon a finding that enforcement of the rights of consumers by private civil action would be so burdensome or expensive as to be impractical. In addition to other penalties and enforcement provisions provided by law, any person who violates or who procures, aids or abets in a violation of the data breach notification law will be subject to a penalty of not more than $1,000 per violation, but no more than $500,000 total, which will be paid to the General Fund of the State Treasury.
Tennessee	Any customer of the information holder who is a person or business entity may institute a civil action to recover damages and enjoin the person or business entity from further action in violation. However, customers cannot be an agency of the state or any political subdivision of the state. In addition, a violation can subject the violator to a civil penalty of $10,000, $5,000 per day that a person's identity has been assumed, or 10 times the amount obtained or attempted to be obtained through the identity theft, whichever is greater. The attorney general can also seek injunctions and get attorneys' fees. A violation under this statute may also be a violation of the Tennessee Consumer Protection Act.

Source: See Baker Hostetler Law
https://www.bakerlaw.com/files/uploads/documents/data%20breach%20documents/data_breach_charts.pdf.

REFERENCES

1. **Colorado:**
Statute:
http://www.leg.state.co.us/CLICS/CLICS2010A/csl.nsf/fsbillcont3/7772EFE1E998E627872576B700617FA4?Open&file=1330_enr.pdf
Rule: http://www.civhc.org/getmedia/2a315773-cbcd-4f75-805a-759d3cf96888/Rules-Governing-Data-Submissions-to-APCD-2011-08-24.pdf.aspx/

2. **Maine**
Statute: http://www.mainelegislature.org/legis/statutes/22/title22sec8703.html
Rules: https://mhdo.maine.gov/claims.htm

3. **Massachusetts**
Statute: http://chiamass.gov/relevant-regulations-5
Rules: http://chiamass.gov/assets/docs/g/chia-regs/957-8.pdf

4. **Oregon**
Statute: http://www.oregon.gov/oha/ohpr/Pages/Statutes-Health%20Care%20Data%20Reporting.aspx
Rules: http://www.oregon.gov/oha/OHPR/rulemaking/notices/409-025_PermComplete_2.1.13.pdf

5. **Vermont**
Statute: http://www.leg.state.vt.us/statutes/fullsection.cfm?Title=18&Chapter=221&Section=09410
Rules: http://gmcboard.vermont.gov/sites/gmcboard/files/REG_H-2008-01.pdf