Office of Privacy & Data Protection

February 21, 2020

Katy Ruckle, State Chief Privacy Officer

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Background

- Admitted to WSBA 2005
- Started with state in 2006
- Contracts/procurement
- Healthcare

Office of Privacy and Data Protection (OPDP)

Office of Privacy
& Data Protection

RCW 43.105.369

OPDP in the Office of the Chief Information Officer

ESSHB 1783 Considerations:

Coordinate with the OPDP to address cybersecurity and data protection for all data collected by the Office of Equity.

State Office of Cybersecurity

OFFICE OF CyberSecurity STATE OF WASHINGTON

- Provides strategic direction for cybersecurity and protects the state government network from growing cyber threats.
- Detects, blocks and responds to cyberattacks on state networks. Prevent and mitigate threats before damage occurs.
- Builds more secure networks and has teams that can respond on a moment's notice to help agencies deal with cyber threats.

Cybersecurity Relationship to Privacy

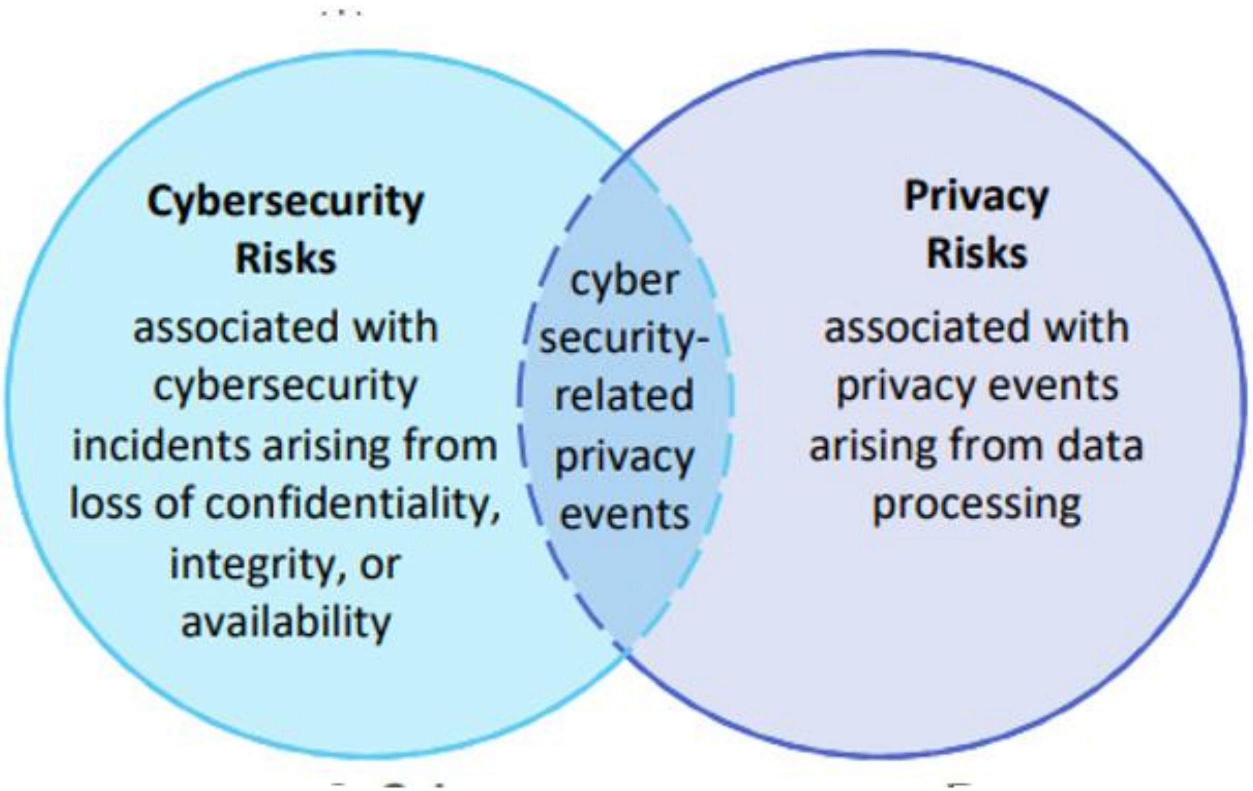
Cybersecurity

- **State Chief Information Security Officer (CISO)**
- Vinod Brahmapuram is Washington State's CISO.
- **Office of the Chief Information Officer IT Security Policies**
- Policy 143: IT Security Incident Communication
- Policy 141.10: Securing Information Technology Assets Standards

Privacy

- **State Chief Privacy Officer (CPO)**
- Katy Ruckle is Washington State's CPO.
- **Office of Privacy and Data Protection Data Stewardship Principles**
- **privacy.wa.gov**

Cybersecurity Relationship to Privacy



Cybersecurity Risks

associated with cybersecurity incidents arising from loss of confidentiality, integrity, or availability

cyber security-related privacy events

Privacy Risks

associated with privacy events arising from data processing

ESSHB1783 Considerations

- When collecting data pursuant to [(d) Data maintenance and establishing performance metrics], the office may not **request** any **PII** from respondents other than **race** and **ethnicity** information identified in (d)(i)(A) of this subsection, in order to protect the data of vulnerable populations.

What is Personally Identifiable Information?

- ESSHB 1783 does not define what **PII** is.
- The proposed Washington Privacy Act (SB 6281)defines "**personal data**" as any information that is linked or reasonably linkable to an identified or identifiable natural person. "Personal data" does not include deidentified data or publicly available information.
- RCW 42.56.590 defines **personal information**

RCW 42.56.590 -
Main changes in legislation from current law:

- Expands definition of Personal Information
- Reduces time for notification of affected individuals from 45 days to 30 days
- Reduces time for notification to the AGO to 30 days
- Specifies more information that the AGO needs to be notified about (see Section 5(7)(a))

Expansion of Personal Information

Now –
Name in combination with:

- SSN;
- Drivers License # or WA ID #;
- Full account number, credit or debit card number, or any required security code, access code, or password that would permit access to an individual's financial account.

After March 1, 2020-
Name in combination with:

- SSN;
- Driver's license # or WA ID #;
- Account number, credit or debit card number, or any other security code, access code, or password that would permit access to an account;
- Full date of birth;
- Private key … that is used to authenticate or sign an electronic record;
- Student, military, or passport ID #
- Health insurance policy # or health insurance ID #;
- Health information;
- Biometric data;
- User name or email address in combination with a password or security answers that permits account access

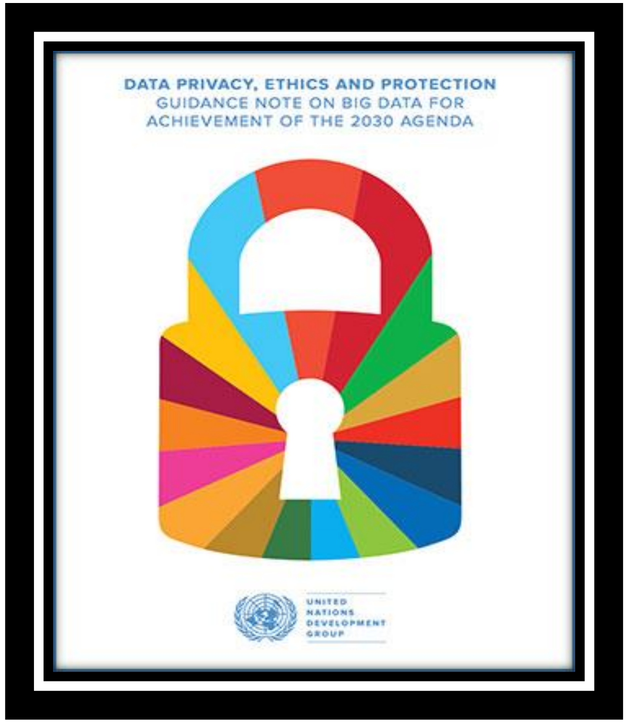
Personal Information (PI) is an individual's first name or first initial and last name in combination with any one or more of the following data elements:

1. SSN;
2. Driver's license # or WA ID #;
3. Account number, credit or debit card number, or any other security code, access code, or password that would permit access to an account;
4. Full date of birth;
5. Private key … that is used to authenticate or sign an electronic record;
6. Student, military, or passport ID #
7. Health insurance policy # or health insurance ID #;
8. Health information;
9. Biometric data (see Chapter 19.375 RCW and Chapter 40.26 RCW);
10. User name or email address in combination with a password or security answers that permits account access*****

*** Does not require first name/initial or last name combination**

Data Stewardship Principles

- DATA RETENTION AND MINIMIZATION
- DUE DILIGENCE FOR COLLABORATORS
- SENSITIVE DATA AND CONTEXTS
- QUALITY AND ACCURACY
- OPEN DATA, TRANSPARENCY, and ACCOUNTABILITY
- DATA SECURITY



DATA PRIVACY, ETHICS AND PROTECTION
GUIDANCE NOTE ON BIG DATA FOR
ACHIEVEMENT OF THE 2030 AGENDA

UNITED
NATIONS
DEVELOPMENT
GROUP

Data Stewardship Principles

DATA RETENTION AND MINIMIZATION

Do we really need it?

- Data access, analysis or other use should be kept to the minimum amount necessary to fulfill its purpose
- Any retention of data should have a legitimate and fair basis, including beyond the purposes for which access to the data was originally granted
- Any data retention should be also considered in light of the potential risks, harms and benefits
- The data should be permanently deleted upon conclusion of the time period needed to fulfill its purpose
- Any deletion of data should be done in an appropriate and secure manner

Data Stewardship Principles

DUE DILIGENCE FOR COLLABORATORS

Do we know our partners?

- Third party collaborators engaging in data use should act in compliance with relevant laws, including privacy laws as well as the highest standards of confidentiality and moral and ethical conduct
- Use a process of due diligence to evaluate the data practices of any potential third party collaborators
- Legally binding agreements for data access and handling should be established – "data sharing agreements"

Data Stewardship Principles

SENSITIVE DATA AND CONTEXTS

Who's it all about?

- Stricter standards of data protection should be used when handling data on vulnerable populations and persons at risk
- It is important to consider that context can turn non-sensitive data into sensitive data. The context in which the data is used (e.g. cultural, geographic, religious, the political circumstances, etc.) may influence the effect of the data analysis on an individual(s) or group(s) of individuals, even if the data is not explicitly personal or sensitive

Data Stewardship Principles

Is it true?

QUALITY AND ACCURACY

- Data should be validated for accuracy, relevancy, sufficiency, integrity, completeness, usability, and coherence, and be kept up to date
- Data quality should be carefully considered in light of the risks that the use of low quality data for decision-making can create for an individual(s) and group(s) of individuals
- Data quality must be assessed for biases to avoid any adverse effects, where practically possible, including giving rise to unlawful and arbitrary discrimination

Data Stewardship Principles

Publish what's public

OPEN, TRANSPARENT & ACCOUNTABLE

- Transparency is a critical element of accountability. Being transparent about data use (e.g. publishing data sets or publishing an organization's data use practices) is generally encouraged

- Except in cases where there is a legitimate reason not to do so, at minimum algorithms used for processing data should be publicly disclosed and described in a clear and non-technical language suitable for a general audience.

- Open data is an important driver of innovation, transparency and accountability. Therefore, whenever possible, the data should be made open, unless the risks of making the data open outweigh the benefits or there are other legitimate bases not to do so.

Data Stewardship Principles

Are we secure?

DATA SECURITY

- Data security is crucial in ensuring data privacy and data protection. Taking into account available technology and cost of implementation, robust technical and organizational safeguards and procedures (including efficient monitoring of data access and data breach notification procedures) should be implemented to ensure proper data management throughout the data lifecycle and prevent any unauthorized use, disclosure or breach of personal data.

- Encrypt personal and sensitive data when transferred to or from any network-connected server. No de-identified data should knowingly and purposely be re-identified, unless there is a legitimate, lawful and fair basis. To minimize the possibility of re-identification, it is recommended that de-identified data not be analyzed or otherwise used by the same individuals who originally de-identified the data.

- Data access should be limited to authorized personnel, based on the “need-to-know” principle. Personnel should undergo regular and systematic data privacy and data security trainings. Prior to data use, vulnerabilities of the security system (including data storage, way of transfer, etc.) should be assessed.

Summary of Concepts

- Office of Privacy an Data Protection
- Cybersecurity vs. Privacy
  - CISO vs. CPO
- Personally identifiable information vs. Personal Information vs. Personal data
- Data Stewardship Principles

Thank you

Questions?