

Purchasing - A Privacy Powerhouse

2021 Training Program



Presented by:

Ashley Summit, Chief Privacy Officer

Lori L. Tarr, Assistant Chief Privacy Officer

Executive Branch

Objectives

- Learn how a partnership between Purchasing and the State Privacy Program provides a risk management function for the state;
- Highlight the West Virginia's State Privacy Program and Executive Branch Privacy Policies;
- Review HIPAA & HITECH Acts and why the Business Associate Addendum is so important for our HIPAA covered agencies;
- Highlight privacy terms in our state contract forms;
- Learn about the Software-as-a-Service Addendum; and,
- Review the Privacy Impact Assessment and its relationship to the SaaS Addendum.

Purchasing and Privacy as Partners in Risk Managers



- Accountability
- Confidentiality

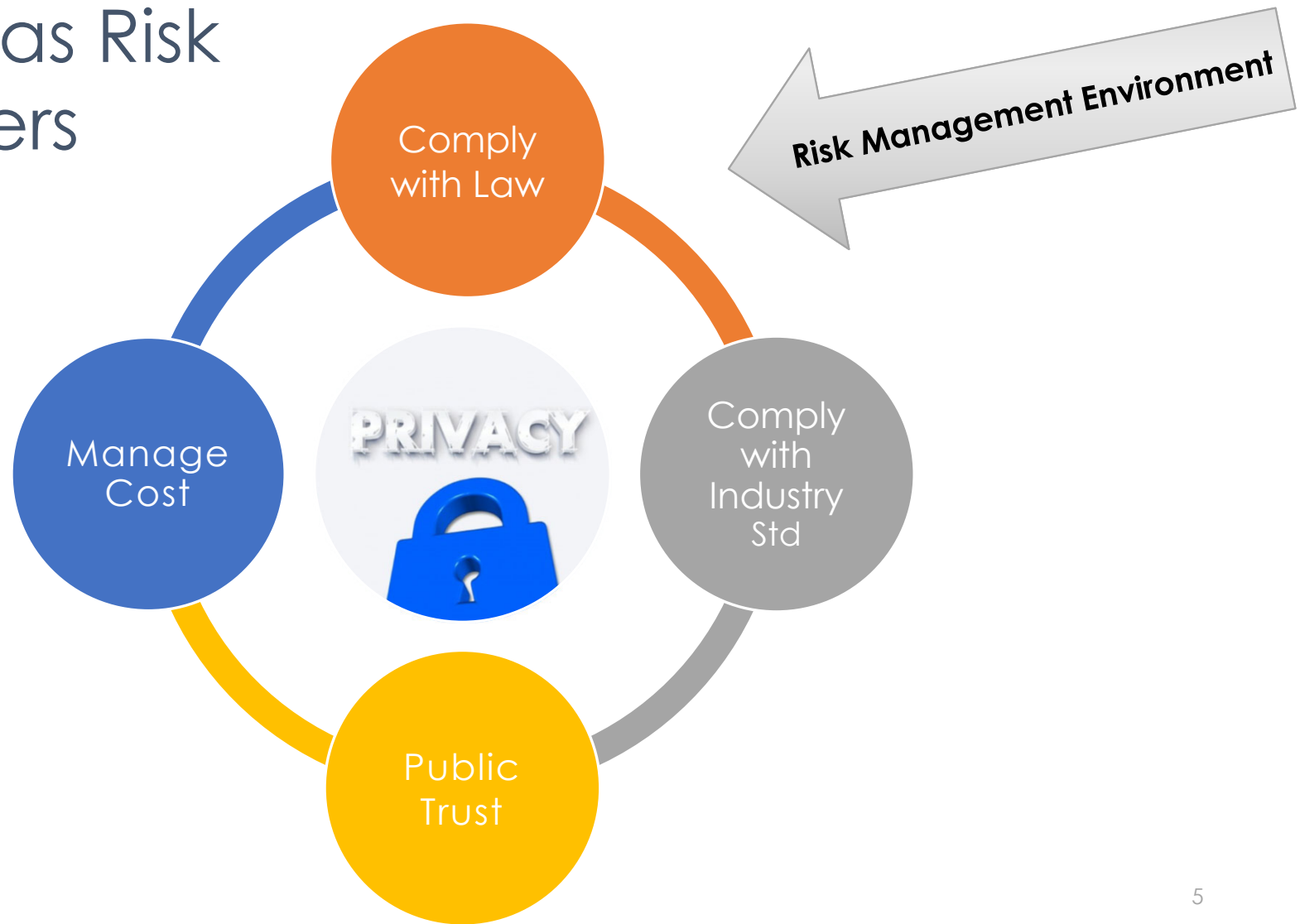
- Reliability
- Security

Purchasing as Risk Managers



- Negligence
- Inequality and insider dealings
- Shoddiness
- Wastefulness

Privacy as Risk Managers





- Executive Order No. 3-17
- State Privacy Office, WV Board of Risk & Insurance Management
- Privacy Management Team
- Privacy Policies

State Privacy Office

- **WV Board of Risk and Insurance Management**

- Ashley Summitt, Chief Privacy Officer

- Leads the Executive Branch's Privacy Program
- Practiced law for 20 years
- Served as Deputy General Counsel and Privacy Officer for Governor's Office, and, General Counsel for the Secretary of State

- Lori Tarr, Assistant Chief Privacy Officer

- Health Care Financial Analyst for 22 years
- Joined the State Privacy Office in December 2016

- Tara Taylor, Administrative Assistant

- Assists in incident response
- Oversees compliance with the online privacy training across the executive branch
- Can't do-it-with-out-her person

WEST VIRGINIA PRIVACY MANAGEMENT TEAM



**Dept. of
Administration**

**Dept. of Arts,
Culture & History**

**Dept. of
Commerce**

**Dept. of
Environmental
Protection**

**Dept. of Health
and Human
Resources**

**Dept. of
Homeland
Security**

**Dept. of
Revenue**

Dept. of Transportation

Dept. of Veterans Assistance

Bureau of Senior Services

Chapter 30 Licensing Boards

Other Constitutional Offices and Higher Education

- State Auditor's Office
- Department of Education
- State Treasurer's Office
- Supreme Court of Appeals
 - Marshall University
 - School of Osteopathic Medicine
- West Virginia University

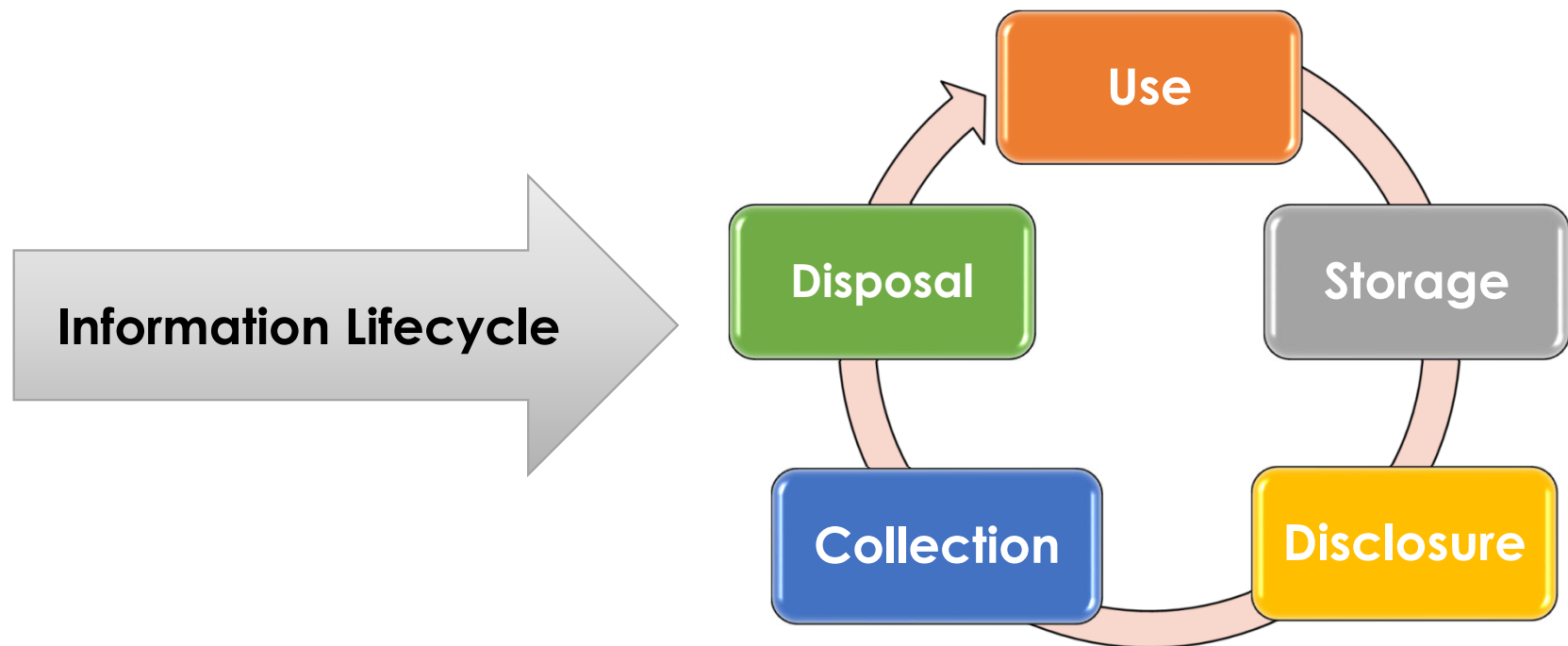
Six Privacy Policies: Compliance is required for all Executive Branch Departments. Consistent with law and regulation.

ACCOUNTABILITY WVEB-P101	Each Department is responsible for maintaining the privacy of PII that it creates, collects, uses, discloses, etc. shall assign roles and responsibilities to ensure application of privacy principles to Personally Identifiable Information (PII).
CONSENT WVEB-P102	Each Department shall provide individuals with a reasonable opportunity to object to the collection, use or disclosure of the PII. A Department does not collect, use or disclose PII in a manner inconsistent with its notice, unless it has first obtained the individual's additional consent for the use or disclosure or the additional use is required by law.
INDIVIDUAL RIGHTS WVEB-P103	When possible, and appropriate, a Department shall rely first on the PII it collects directly from the individual. An individual should be afforded the ability to access and copy his or her PII, request an amendment to the information or the information be annotated. Departments shall provide appropriate means of individual redress, which includes institutional mechanisms to ensure that individuals have a simple and effective way to have their questions answered and concerns addressed.
MINIMUM NECESSARY AND LIMITED USE WVEB-P104	Departments shall limit the collection, and disclosure of PII to their legal authority. Additionally, Departments should only collect or disclose those elements of PII that are reasonably needed to accomplish a legitimate Departmental objective, except where law or public policy directs otherwise.
NOTICE WVEB-P105	Departments shall be open regarding the authority for collecting PII; the purpose of the collection; the location of the entity maintaining the PII; with whom the PII may be shared and why; rights an individual has; and the Department's policies procedures, standards, and practices with regard to PII.
SECURITY SAFEGUARDS WVEB-P106	Departments must implement the appropriate management, operational, physical and technical controls to preserve the privacy, confidentiality, integrity and accessibility of PII. The security safeguards shall be designed to protect the PII from anticipated threats or hazards, and unauthorized access, use or disclosure. Security should be proportional with the greatest effort applied to the PII that could result in the greatest harm if compromised.

What is privacy?

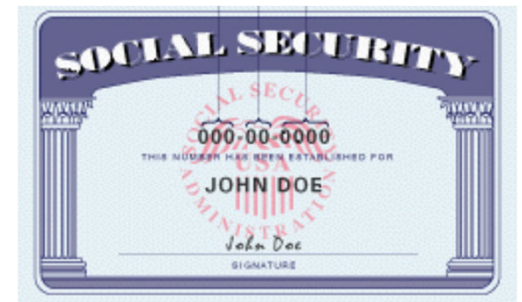
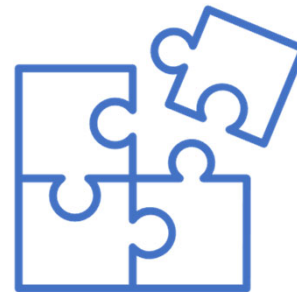
Privacy is about **data** privacy, which means using and disclosing data appropriately.

Rights and obligations of individuals and organizations with respect to processing of personal information. GAPP



WHAT IS PERSONALLY IDENTIFIABLE INFORMATION (PII)?

- All information that identifies, or can be used to identify, locate, or contact an individual.
- PII is contained in public and non-public records.
- Includes: PHI, FTI, PCI



Why protect privacy?



The threats to individuals and organizations are real. Globally. That means us too.

News Headlines

Surveillance Company Verkada Hacked

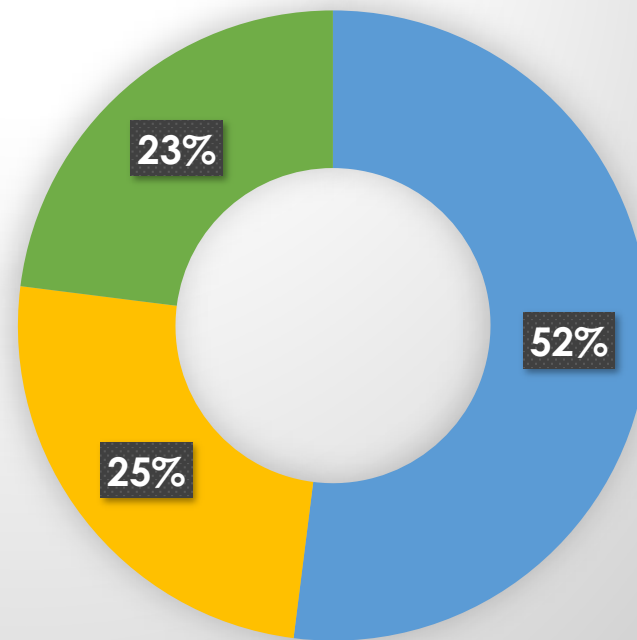
Affects of Accellion Data Breach Spread

SolarWinds Victim of Massive Attack



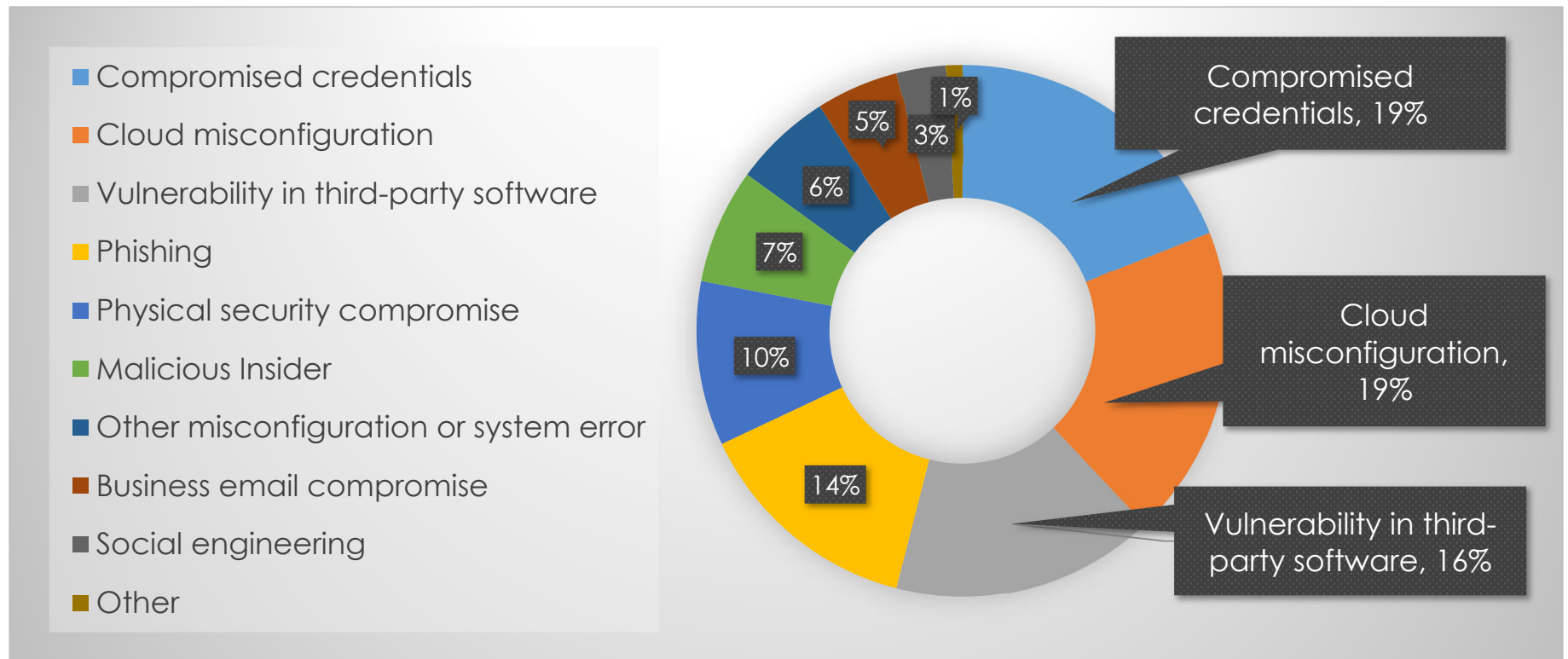
Breach Root Cause of Breaches

- Malicious or criminal attack
- System glitch
- Human error



Source: 2020 Cost of a Data Breach Report, Ponemon Institute, IBM Security

Malicious data breach root causes



Source: 2020 Cost of a Data Breach Report, Ponemon Institute, IBM Security

Why protect privacy?



Data and security breaches are expensive

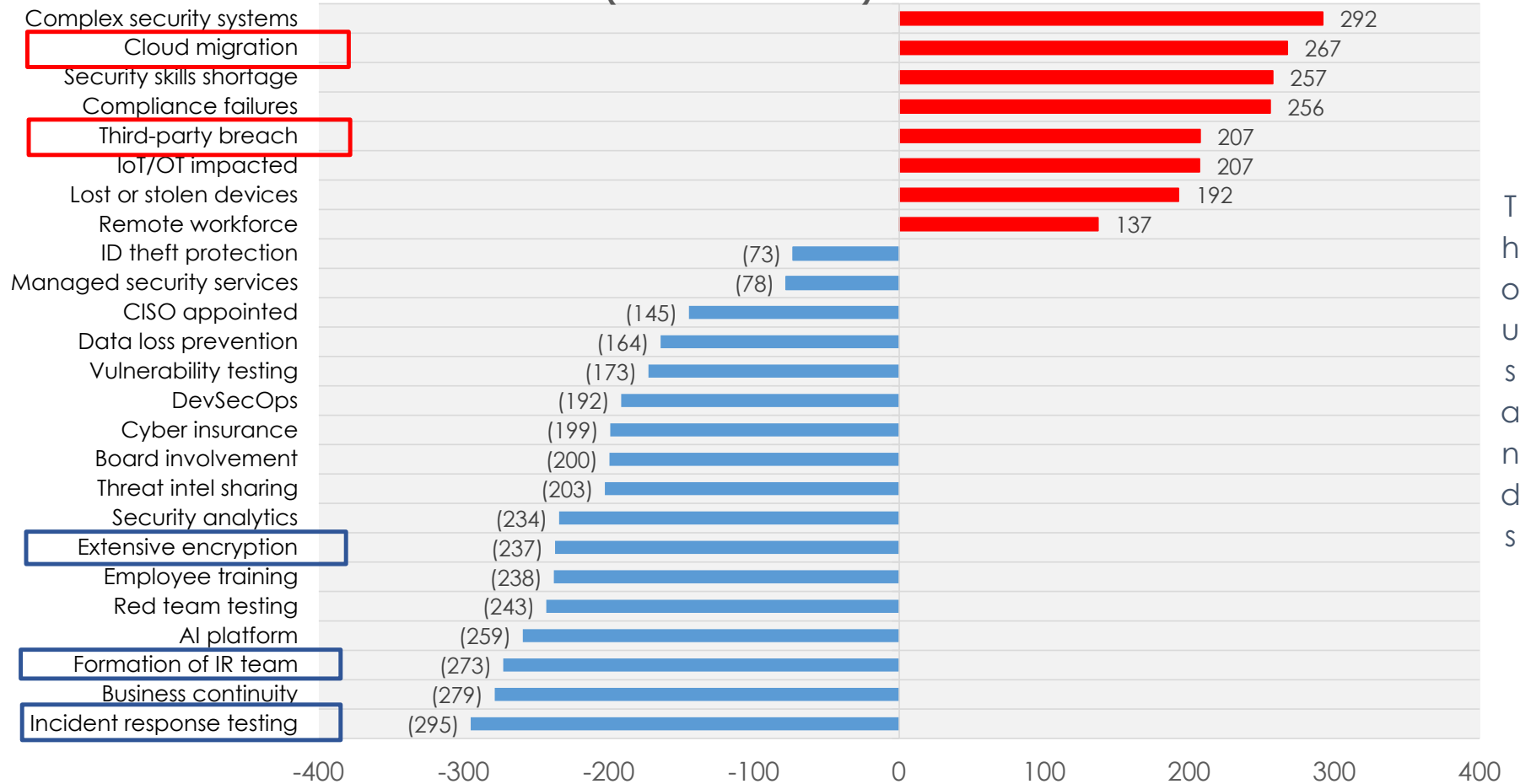
United States:

- Average total cost per breach*: \$8.64 million
- A 5.3% increase from 2019 to 2020
- Does not include mega breaches

Civil and criminal penalties, including personal liability for criminal privacy violations

Sources: Ponemon Institute, 2020 Cost of Data Breach Report. *Global costs

Factors that Increase and (Decrease) Costs of a Data Breach (In Thousands)



Source: 2020 Cost of a Data Breach Report,
Ponemon Institute, IBM Security

Why protect privacy?

Public Trust

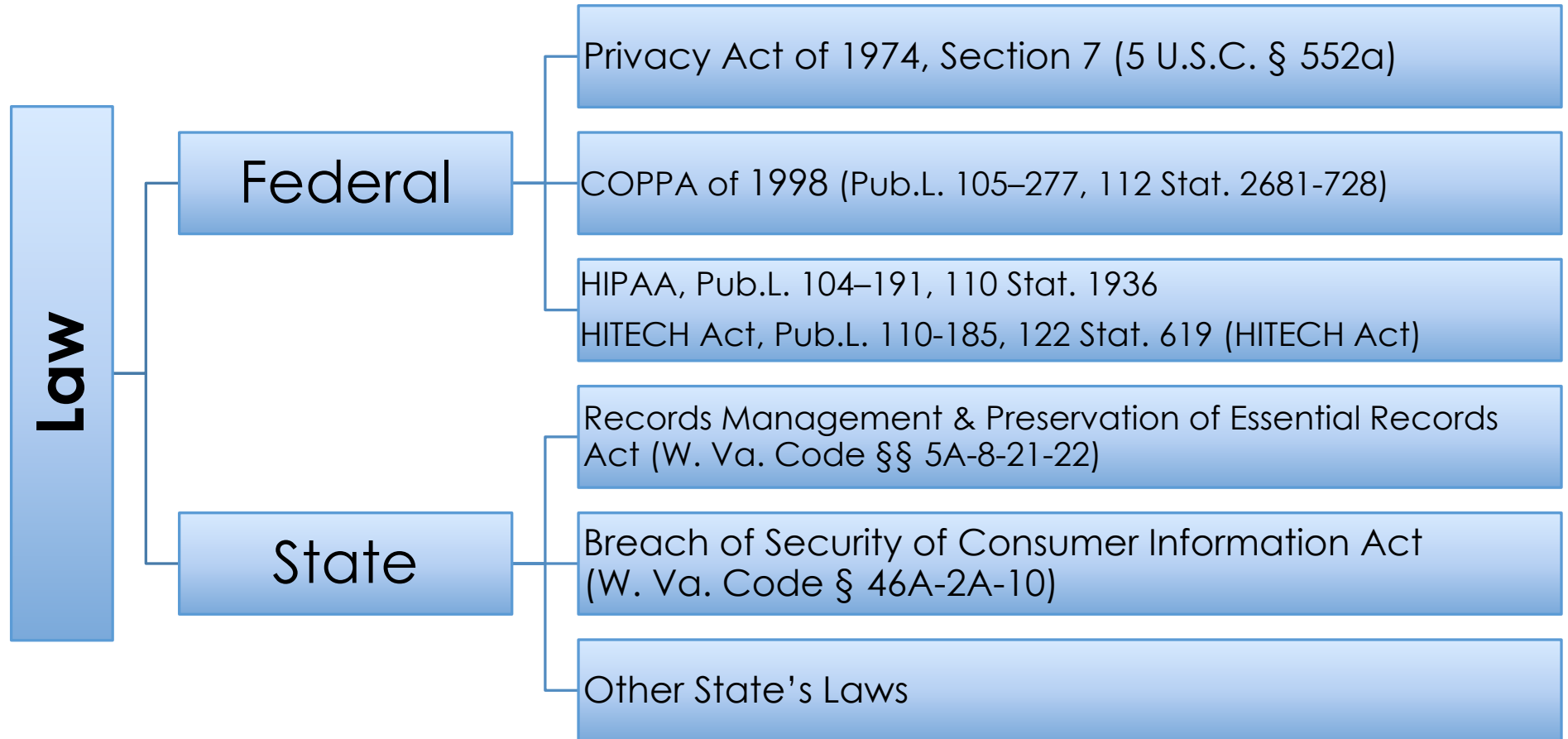
- Duty to provide services
- Citizens have no option to shop around – they are required to provide personal information to the government.
- We have an obligation to protect the information entrusted to us.

Reputational Harm

- Bad press
- Legislative scrutiny



Why protect privacy?



State Law - Records Management & Preservation of Essential Records Act (W. Va. Code §§ 5A-8-21-22)

- Requires state agencies to safeguard the SSN.
- Exempts SSN from FOIA and prohibits release to non-governmental entities, unless authorized by law.
- Exempts disclosure of certain PII for the State workforce:
 - home address,
 - SSN,
 - credit or debit card numbers,
 - driver's license number,
 - marital status
 - maiden name.

Updated by SB 470 – Daniel's Law

- Protection of personal information of active, formerly active or retired judicial officers, prosecutors and law enforcement officers.
- Applied to state or local governmental agencies, agency must get prior written permission to disclose a home address or unpublished home or personal telephone number.
- To violate this law, state and local governmental agencies must disclose the information KNOWINGLY if they will violate the law.
- Does not prohibit disclosure if disclosed by state or federal law.

SB 587 – Prohibited Contract Clauses

- Passed in the 2021 Legislature April 2, and in effect from passage.
- §5A-3-62 Prohibits a variety of contract clauses- are VOID
- Important to privacy
 - (12) Permit assignment of contracts without consent from the state
 - (13) Treat information as confidential contrary to the state's disclosure responsibilities
 - (14) Agree to unsigned third-party terms and conditions
 - (16) Give up ownership right or right of interest in data to be collected by the vendor.

State Law - State Breach Code - §46A-2A-101 Article 2A.

- Unauthorized access to Personal Information that is
 - Maintained within a computer database
 - First name, or first initial, and last name linked to one or more of the following:
 - Social Security Number
 - Driver's License Number (or State ID Card issued in lieu of Driver's License)
 - Financial account number, credit or debit card number in combination with security or access code or password *that allows access to these accounts.*
- Requires notice to individual if high risk of harm



Other Federal Laws

- Internal Revenue Code - 26 U.S. Code § 7213
- Federal Education Rights and Privacy Act
- Driver's Privacy Protection Act of 1994

Federal HIPAA and HITECH Acts

- Health Insurance Portability and Accountability Act of 1996
- The Health Information Technology for Economic and Clinical Health Act of 2009

Privacy Rule

Security Rule

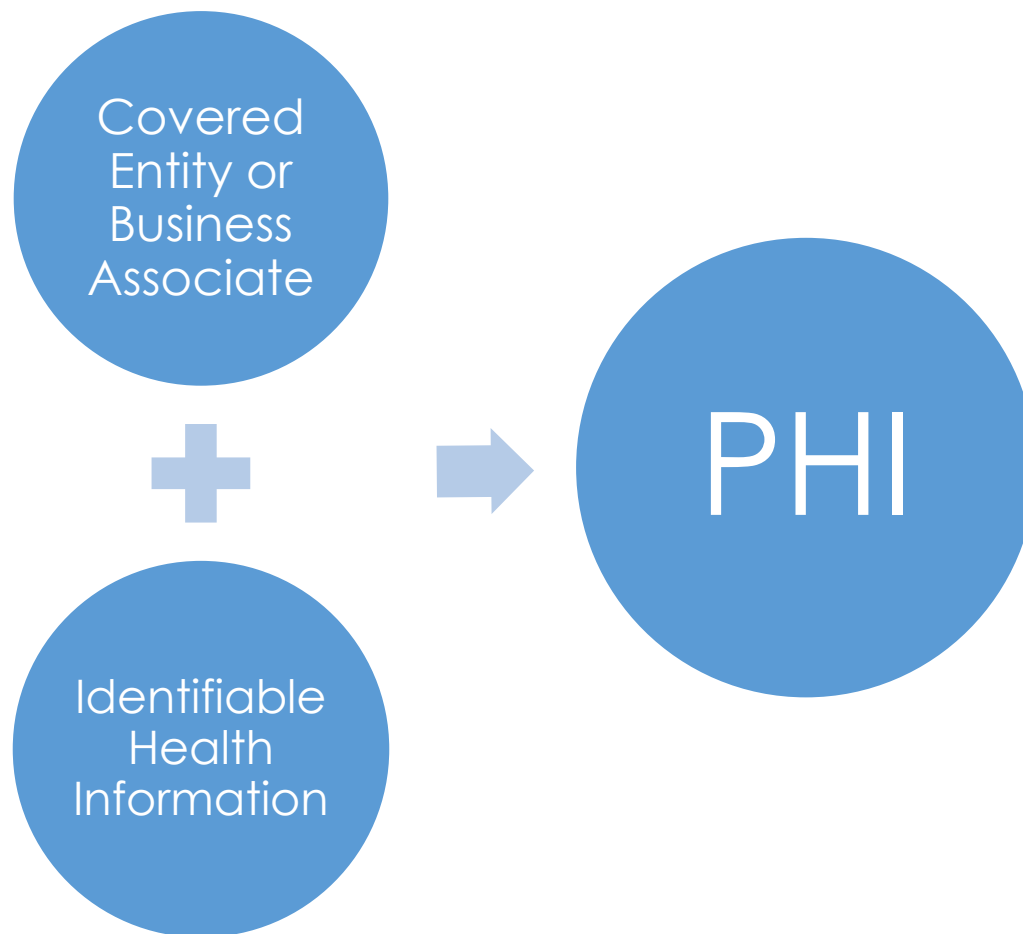
Breach
Notification
Rule

Enforcement
Rule

HIPAA Protects PHI

- Protected Health Information (PHI)
 - A subset of PII – Personally Identifiable Information
 - Individually identifiable health information maintained or transmitted by a covered entity or business associate
- In any form or media – electronic, paper or oral
- Relates to an individual's:
 - Physical or mental condition
 - Provision of health care to the individual, or
 - Payment for the provision of health care
 - Past, present or future

Not all health information is PHI



HIPAA and HITECH Act

- Applies to:
 - **Covered Entities** - health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form
 - **Business Associates** – a person or entity that performs functions or activities that involve protected health information
- Mandated use of Business Associate Agreements by Covered Entities with all Business Associates
- Expanded the responsibility and liability of breaches for both the Covered Entities and Business Associates.

HIPAA/HITECH – Departments/Programs

- Components of Covered Entities and Business Associates
 - PEIA – Covered Entity
 - Department of Health and Human Resources – Hybrid
 - Covered Components include:
 - Medicaid
 - State-owned Hospitals
 - State-owned Long-term Care Facilities
 - Department of Veteran's Assistance – Covered Entity
 - WVOT - Business Associate
 - Bureau of Senior Services – Business Associate
- Contact your Department Privacy Officer to determine coverage: <https://privacy.wv.gov/about/Pages/default.aspx>

Common types of business associates and services

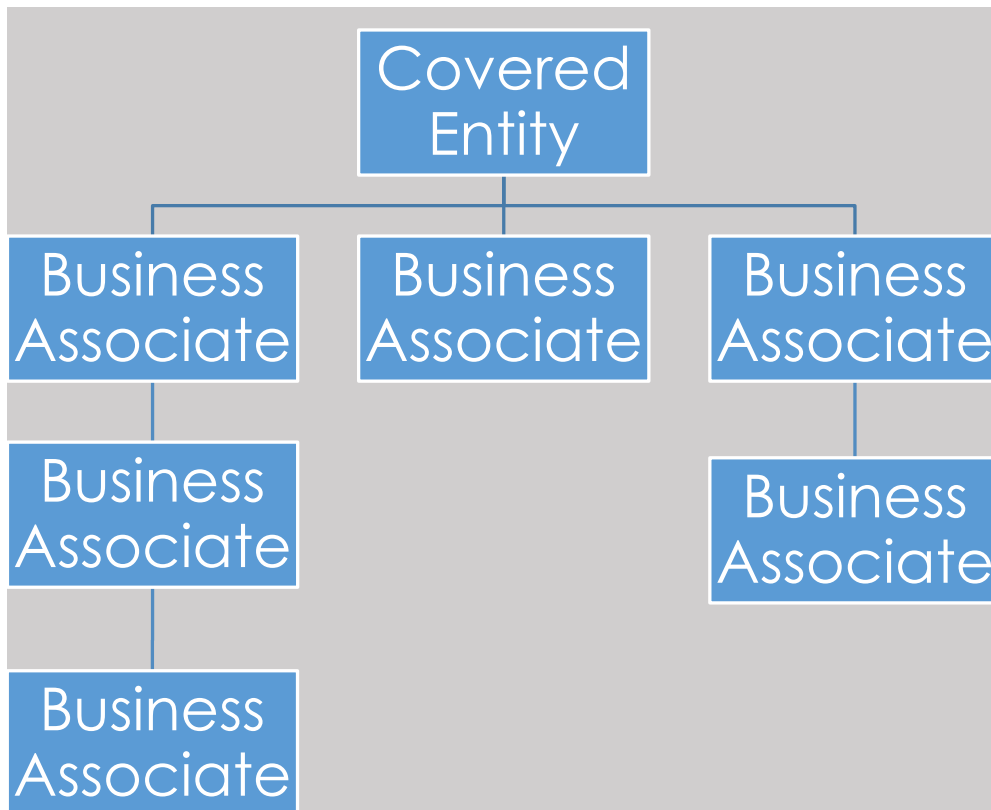
Business Associate Services

- Accounting
- Actuarial
- Administrative
- Consulting
- Data analysis
- Financial
- Legal
- Management

Business Associate Functions

- Bill and claims processing
- Benefit management
- Copy services
- Data aggregation for analysis
- Data storage – including Cloud computing
- Health Information Organizations
- Medical transcription services
- Pharmacy benefits managers
- Practice management
- Quality assurance
- Utilization review services

HIPAA and the Scope of the BAA



- Covers Business Associates of Business Associates - all the way down the chain
- Responsibility cannot be offloaded by Covered Entities to its Business Associates
- Both types of entities are responsible

Enforcement: Office of Civil Rights

May result in *civil* and *criminal* penalties.

Civil Penalty Tiers	Minimum (each violation)	Maximum (each violation)	Total (Identical violations / CY)
Did not know of violation	\$119	\$59,522	\$1,785,651
Violation due to reason cause, not willful neglect	\$1,191	\$59,522	\$1,785,651
Violation due to willful neglect, but corrected	\$11,904	\$59,522	\$1,785,651
Violation due to willful neglect and not corrected	\$59,522	\$1,785,651	\$1,785,651

Source: <https://www.tax.thomsonreuters.com> – most recent update January 17, 2020

Criminal Enforcement: OCR/DOJ

- Criminal Penalties (DOJ):
 - Willful violations - fines
 - \$50,000 (minimum)
 - \$250,000 (maximum)
 - Willful violations – prison
 - Negligence – up to 1 year
 - Acquisition of PHI under false pretenses – 5 years (maximum)
 - Acquisition of PHI for personal gain – 10 years (maximum)
- Pursuant to HITECH, state attorneys general are also permitted to bring civil actions and recover monetary awards that may be shared with harmed individuals.
- Disciplinary action may be taken against workforce members as outlined in the State's personnel, security and privacy policies.

Employees are
subject to HIPAA
sanctions.



30. Purchasing Master Terms and Conditions: Purchasing Master Terms and Conditions

General Terms and Conditions - Term #30:

30. PRIVACY, SECURITY, AND CONFIDENTIALITY: The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the Agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures, and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in <http://www.state.wv.us/admin/purchase/privacy/default.html>.

- Confidentiality from vendor workforce
- Vendor compliance with confidentiality and security requirements
- Link to Purchasing's Privacy and Confidentiality Webpage



12. Agency Master Terms and Conditions: Agency Master Terms and Conditions

General Terms and Conditions - Term #29:

29. PRIVACY, SECURITY, AND CONFIDENTIALITY: The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the Agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures, and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in <http://www.state.wv.us/admin/purchase/privacy/default.html>

- Confidentiality from vendor workforce
- Vendor compliance with confidentiality and security requirements
- Link to Purchasing's Privacy and Confidentiality Webpage

Privacy and Confidentiality Webpage



Privacy and Confidentiality

The purpose of this web page is provide links to policies and information regarding privacy and confidentiality.

Privacy of Information Collected: The Purchasing Division is required to collect certain information as stated in *West Virginia Code* §5A-3-12, other applicable sections of the *West Virginia Code*, the Vendor Registration and Disclosure Statement forms, and other documents to facilitate the state bidding and contract administration processes. That information is generally obtained by the Purchasing Division through the Vendor Registration and Disclosure Statement form or vendors' submitted responses to solicitations, but may be obtained in other forms and formats. All information collected is stored in a secure environment, but unless specifically protected under state law, any information provided to the Purchasing Division may be inspected by or disclosed to the public.

To view and print some documents and pages, you may need Adobe Reader installed on your PC. It is a free download.



[Business Associate Addendum Notice:](#) If you process protected health information on behalf of the State of West Virginia and are considered a business associate, this notice applies to you. All others please disregard.

[HIPAA Business Associate Addendum](#)

[West Virginia Privacy Statement:](#) Pertains to the use of state government web sites.

[Notice of Agency Confidentiality Policies:](#) Serves to inform vendors holding state contracts as to the types of information that need to be safeguarded and their responsibilities.

From Purchasing's Homepage

- [Privacy Information](#) link, bottom of homepage
- Business Associate Addendum
- Notice of Agency Confidentiality Policies

Notice of Agency Confidentiality Policies

Notice of State of West Virginia

Confidentiality Policies and Information Security Accountability Requirements

- Vendor notification required of suspected data security incident or breach
- Vendor to get agency privacy policies, when applicable
- Limits use of personal information to the purpose of the contract
- Denies data ownership by vendor
- Costs associated with breach borne by vendor
- Governs the acquisition process of PII by vendor
- Requires encryption

Vendor Resource Center
<http://www.state.wv.us/admin/purchase/vrc/hipaa.html>

OR

Privacy and Confidentiality
Webpage
<https://www.state.wv.us/admin/purchase/privacy/default.html>

HIPAA Business Associate Addendum

WV STATE GOVERNMENT

HIPAA BUSINESS ASSOCIATE ADDENDUM

This Health Insurance Portability and Accountability Act of 1996 (hereafter, HIPAA) Business Associate Addendum ("Addendum") is made a part of the Agreement ("Agreement") by and between the State of West Virginia ("Agency"), and Business Associate ("Associate"), and is effective as of the date of execution of the Addendum.

The Associate performs certain services on behalf of or for the Agency pursuant to the underlying Agreement that requires the exchange of information including protected health information protected by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111-5) (the "HITECH Act"), any associated regulations and the federal regulations published at 45 CFR parts 160 and 164 (sometimes collectively referred to as "HIPAA"). The Agency is a "Covered Entity" as that term is defined in HIPAA, and the parties to the underlying Agreement are entering into this Addendum to establish the responsibilities of both parties regarding HIPAA-covered information and to bring the underlying Agreement into compliance with HIPAA.

Whereas it is desirable, in order to further the continued efficient operations of Agency to disclose to its Associate certain information which may contain confidential individually identifiable health information (hereafter, Protected Health Information or PHI); and

Whereas, it is the desire of both parties that the confidentiality of the PHI disclosed hereunder be maintained and treated in accordance with all applicable laws relating to confidentiality, including the Privacy and Security Rules, the HITECH Act and its associated regulations, and the parties do agree to at all times treat the PHI and interpret this Addendum consistent with that desire.

NOW THEREFORE: the parties agree that in consideration of the mutual promises herein, in the Agreement, and of the exchange of PHI hereunder that:

1. **Definitions.** Terms used, but not otherwise defined, in this Addendum shall have the same meaning as those terms in the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

- a. **Agency Procurement Officer** shall mean the appropriate Agency individual listed at: <http://www.state.wv.us/admin/purchase/vrc/agencyli.html>.

Tips for Procurement Officers as Privacy Gatekeepers

General Privacy

- Ensure that Privacy, Security and Confidentiality Term is in RFP (4.1)
- When vendor will receive your agency's PII, give the vendor your privacy and security policies (4.2)
- If you are notified that a vendor has had an incident or breach, report it immediately at the OT portal (4.4.2.3)
- If vendor is receiving agency PII, ensure that vendor gives agency a signed acknowledgement (4.6)

HIPAA/HITECH

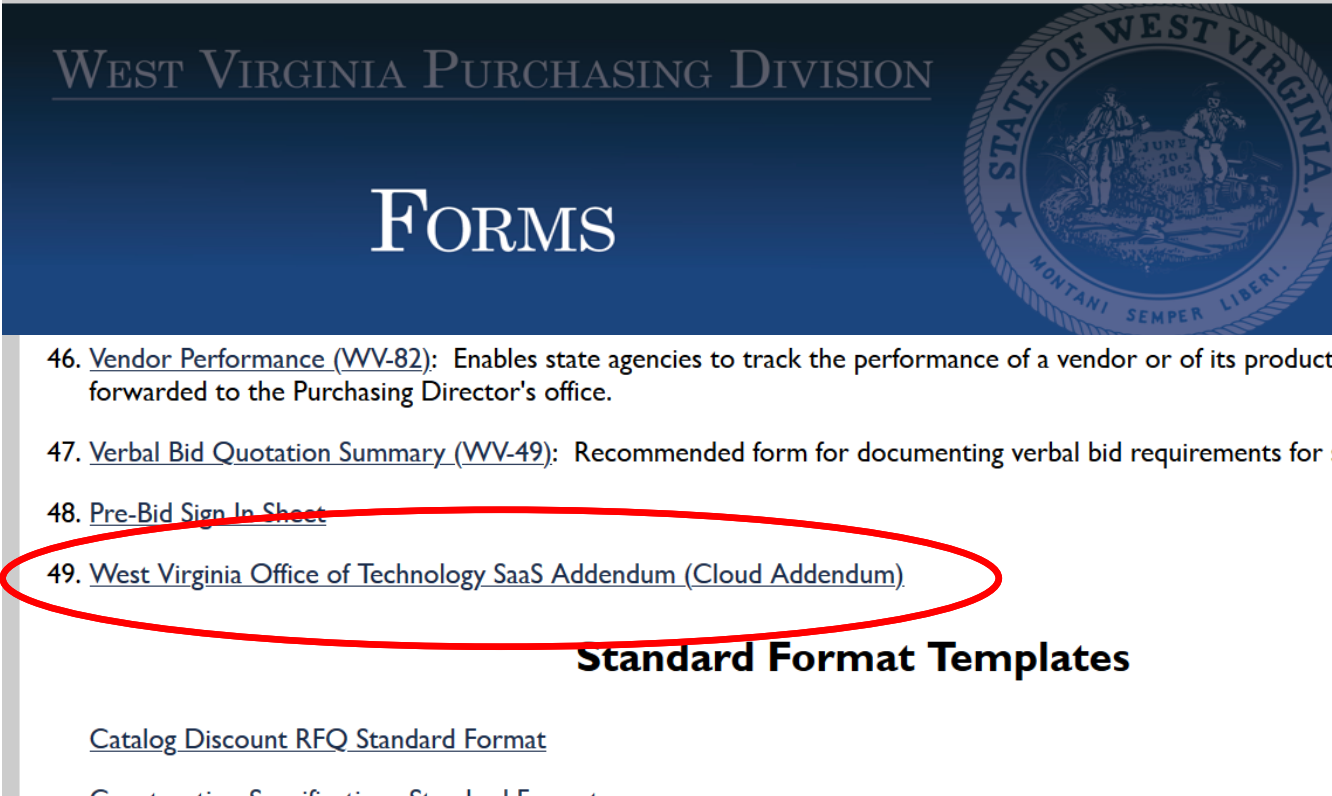
- Use Business Associate Addendum if agency is HIPAA impacted and vendor will process PHI
- Complete Appendix A, detailing type of PHI
- If vendor notifies you of a subcontractor, send to department privacy officer (3.h)
- If vendor notifies you that it does not want to encrypt, send the notification to your department privacy officer ASAP. Agency has 10 days to review and determine prior to contract signing. (3.k)
- If you are notified that a vendor has had an incident or breach, report it immediately at the OT portal (3.l)

Incident Reporting Process

- File an Incident Report through the WVOT portal
 - State Privacy Office website → Incident Response page
 - <https://apps.wv.gov/ot/ir/> (address likely to change in 2021)
- Report should be made as soon as possible, even if **all** information is not yet known.
- Do not include actual PII or PHI in the report – only provide types of PII or PHI that might be involved – if known.


Software-as-a-Service Addendum

<http://www.state.wv.us/admin/purchase/forms.html>



WEST VIRGINIA PURCHASING DIVISION

FORMS



46. Vendor Performance (WV-82): Enables state agencies to track the performance of a vendor or of its product; forwarded to the Purchasing Director's office.

47. Verbal Bid Quotation Summary (WV-49): Recommended form for documenting verbal bid requirements for s

48. Pre-Bid Sign In Sheet

49. West Virginia Office of Technology SaaS Addendum (Cloud Addendum)

Standard Format Templates

Catalog Discount RFQ Standard Format

Construction Specifications Standard Format

Software-as-a-Service Defined

- The capability to use a vendor's application, which is running on a cloud infrastructure.
- The applications are accessible through an interface such as a Web browser (e.g., Web-based email) or a program interface.
- The consumer (state agency) does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities.
- Agency may control limited user-specific application configuration settings

■ Common uses for the SaaS model:

- Office software
- CAD software
- Enterprise resource planning
- Human resource management
- Learning management systems
- Geographic information systems
- Service desk management

Source: https://en.wikipedia.org/wiki/Software_as_a_service

■ Common examples of SaaS:

- Salesforce.com
- Microsoft Office 365
- DocuSign
- Dropbox
- Zendesk
- Slack

Source: <https://getnerdio.com/academy/10-popular-software-service-examples/>

Key Points:

WVOT Software-as-a-Service Addendum

- **Term 2. Data Ownership:** The public jurisdiction will own all right, title and interest in its data that is related to the services provided by this contract.
 - The service provider shall not access user accounts or data, except for certain circumstances.
- **Term 3. Data Protection and Privacy:** Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time.

Key Points:

WVOT Software-as-a-Service Addendum

■ **Term 3. Data Protection and Privacy:**

- e) All **personal data** shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of the personal data.
- f) The service provider shall encrypt all **non-public data** at rest and in transit, in accordance with recognized industry practice (unless otherwise stipulated).
 - The public jurisdiction shall identify data it deems as non-public data to the service provider.

- **Term 23. Encryption of Data at Rest:** Service provider shall ensure encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all personal data.

- (FIPS = Federal Information Processing Standards)

Key Points:

WVOT Software-as-a-Service Addendum

■ **Term 3. Data Protection and Privacy:**

- h) The service provider shall not use or disclose any information collected...for any purpose other than fulfilling the service.
- i) **Data Location.** For non-public data and personal data:
 - Data center services must be located in the U.S.
 - Storage of data shall be located solely in data centers in the U.S
 - Must not be stored on portable devices
 - Exceptions - Acceptable alternative data center location
 - A country that is identified as providing equivalent or stronger data protection than the US, in terms of both regulation and enforcement.
 - DLA Piper's Privacy Heatmap shall be utilized for this analysis and may be found at <https://www.dlapiperdataprotection.com/index.html?t=worldmap&c=US&c2=IN>.
to

Key Points:

WVOT Software-as-a-Service Addendum

■ **4. Security Incident or Data Breach Notification:**

- The service provider shall inform the public jurisdiction of any confirmed security incident or data breach
- Incident Response, Security Incident Reporting Requirements – 24 hours max

■ **5. Breach Responsibilities:** This section includes

- Communication requirements with agencies
- Acceptance of responsibility for privacy and security incidents, and management of incidents, for violations of contract requirements.

Key Points:

WVOT Software-as-a-Service Addendum

■ **Term 7. Termination and Suspension of Service:**

- a) Termination of the contract...an orderly return of data within the time period and format specified in the contract.
- e) The service provider shall securely dispose of all requested data in all of its forms, such as disk, CD/ DVD, backup tape and paper.
 - Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods.
 - Certificates of destruction shall be provided to the public jurisdiction

SaaS Addendum – Appendix A

■ Appendix A –

- Completed prior to execution of Addendum.
- Output for Appendix A – Source is Privacy Impact Assessment – Tab 7
- Any project that needs a SaaS must do a Privacy Impact Assessment

Appendix A

(To be completed by the Agency's Procurement Officer prior to the execution of the Addendum, and shall be made a part of the Addendum. Required information not identified prior to execution of the Addendum may only be added by amending Appendix A and the Addendum, via Change Order.)

Name of Service Provider/Vendor: _____

Name of Agency: _____

Agency/public jurisdiction's required information:

1. Will restricted information be processed by the service provider?
Yes ☐
No ☐
2. If yes to #1, does the restricted information include personal data?
Yes ☐
No ☐
3. If yes to #1, does the restricted information include non-public data?
Yes ☐
No ☐
4. If yes to #1, may the service provider store public jurisdiction data in a data center in an acceptable alternative data center location, which is a country that is not the U.S.?
Yes ☐
No ☐
5. Provide name and email address for the Department privacy officer:

Name: _____

Privacy Impact Assessment?

Useful as a privacy management tool to evaluate the implications of privacy in




New
Information
Systems

New
Technology
Purchases

Significantly
Modified
Information
Systems

Privacy Impact Assessment

Instructions – Tab 1

	A	B	C	D	E	F	G	H	I
1	 <div>Instructions for the West Virginia Executive Branch Privacy Impact Assessment (PIA)</div>								
2									
3									
4									
5									
6	FILING INFORMATION								
7									
8	<ul style="list-style-type: none">• After completing this form, submit it by e-mail to the following people:								
9	<ul style="list-style-type: none">• Lori Tarr - Assistant Chief Privacy Officer, State Privacy Office lori.l.tarr@wv.gov								
10	<ul style="list-style-type: none">• Tara Taylor - Administrative Assistant, State Privacy Office tara.l.taylor@wv.gov								
11	<ul style="list-style-type: none">• Cyber Security Office, WV Office of Technology CSO@WV.GOV								
12	<ul style="list-style-type: none">• Procurement Officer								
13	<ul style="list-style-type: none">• Department Privacy Officer								
14	<ul style="list-style-type: none">• Security Officer (when applicable)								
15	<ul style="list-style-type: none">• Agency Privacy Officer (when applicable)								
16									
17	PIA INFORMATION								
18									
19	<ul style="list-style-type: none">• Complete <u>all</u> six of the numbered worksheets unless you only are required to complete through worksheet 2 - the Threshold Analysis tab. See explanation below regarding completion of Tab 7. Appendix A.								
20	<ul style="list-style-type: none">• This workbook is protected from changes. Do not unprotect or change the format in any way.								
21	<ul style="list-style-type: none">• Tab key can be used for easiest navigation through unlocked cells.								
22	<ul style="list-style-type: none">• Use the mouse to hover over checkboxes.								
23	<ul style="list-style-type: none">• Look for the action items. These are tips that may be revealed, depending on your answers, that will point you to relevant policies. The information is provided next to your answer and in most cases is formatted like this box. For your convenience, links to privacy and security policies are provided here:								
24	<ul style="list-style-type: none">• State Privacy Policies: Privacy Policies								
25	<ul style="list-style-type: none">• Cyber Security Policies: Security Policies								
26									
27	I. GENERAL INFORMATION								
28	<ul style="list-style-type: none">• Provide general contact and project information on Tab 1. Contact information should be submitted for								
29									
30									
31									
32									
33									
34									
35									
36									
37									
38									
39									
40									
41									
42									
43									
44									
45									
46									
47									
48									
49									
50									

General Information – Tab 2

Section 1: General Information	
INDIVIDUAL COMPLETING THIS FORM	
FIRST NAME	<input type="text"/>
LAST NAME	<input type="text"/>
ROLE/TITLE	<input type="text"/>
DEPARTMENT	<input type="text"/>
DIVISION/AGENCY	<input type="text"/>
PHONE NUMBER	<input type="text"/>
EMAIL ADDRESS	<input type="text"/>
PROJECT INFORMATION	
PROJECT MANAGER	<input type="text"/>
PROJECT NAME	<input type="text"/>
PROJECT START DATE (mm/dd/yy)	<input type="text"/>
Is the project an information system, with a system number provided by the WV Office of Technology? (Select Yes or No) <input type="text"/>	
If Yes, enter number:	<input type="text"/>
DEPARTMENT PRIVACY OFFICER	
PRIVACY OFFICER	<input type="text"/>
DEPARTMENT	<input type="text"/>
PHONE NUMBER	<input type="text"/>
EMAIL ADDRESS	<input type="text"/>
DEPARTMENT SECURITY OFFICER*	
*Use if your department or agency has a designated Information Security Officer or Chief Information Officer.	
SECURITY OFFICER	<input type="text"/>
Instructions 1. General Information 2. Threshold Analysis 3. Data Classification 4. Collection, Use & Storage	



SaaS Appendix A Output

Linked input from
Worksheet 3 – Q 1-4

Linked input from
Worksheet 1 – Q5

Manual Input - Q6

	A	B	C	D	E	F	G	H	I	J
1	Procurement Officer Report									
2	for									
3	Appendix A of the Software as a Service Addendum									
4										
5	Agency/public jurisdiction's required information - Questions 1 - 6									
6										
7										
8										
9	1.	Will restricted information be processed by the service provider?								<input type="text"/>
10										
11	2.	If yes to #1, does the restricted information include personal data?								<input type="text"/>
12										
13	3.	If yes to #1, does the restricted information include non-public data?								<input type="text"/>
14										
15	4.	If yes to #1, may the service provider store public jurisdiction data in a data center in an acceptable alternative data center location, which is a country that is not the U.S.?								<input type="text"/>
16										
17										
18										
19										
20										
21										
22										
23	5.	Provide the name and email address of the Department Privacy Officer								
24										
25	Name:	<input type="text"/>								
26										
27	Email:	<input type="text"/>								
28										
29										
30	6.	Provide the name and contact information for vendor's employee who shall serve as the public jurisdiction's primary security contact:								
31										
32										
33	Name:	<input type="text"/>								
34										
35	Email:	<input type="text"/>								
36										
37	Phone:	<input type="text"/>								
38										
39										

Final Tips

- Develop a relationship with Department Privacy Officer.
- Ask your Department Privacy Officer to send you a link to your privacy and security policies, so that you have the right information to send to the vendor.
- Determine whether your agency is covered by HIPAA – covered entity or business associate.
- Work with Project Managers and Departmental Privacy Officer to complete Privacy Impact Assessment (PIA) for new technology or modification of old tech.

Resources: New website coming



- Current:
www.privacy.wv.gov
- Soon:
www.brim.wv.gov/privacy

- Report a privacy incident → **Incident Response** page.
- PIA → **Privacy Impact Assessment** Page
- Locate your department/agency privacy officer → **Contact Us** page

Utilize Purchasing Division contract forms:

- General Terms and Conditions
 - Purchasing - <http://www.state.wv.us/admin/purchase/TCP.pdf>
 - Agency Delegated Procurements - <http://www.state.wv.us/admin/purchase/TCA.pdf>
- Purchasing Privacy and Confidentiality Webpage <http://www.state.wv.us/admin/purchase/privacy/default.html>
 - HIPAA Business Associate Addendum - <http://www.state.wv.us/admin/purchase/vrc/WvBaaAgEffectiveJun2013.pdf>
 - Notice of Agency Confidentiality Policies: <http://www.state.wv.us/admin/purchase/privacy/NoticeConfidentiality.pdf>
- Purchasing Forms - <http://www.state.wv.us/admin/purchase/forms.html>

Questions?



Contact Information

Board of Risk and Insurance Management

1124 Smith Street, Suite 4300

Charleston, WV 25301

Phone 304.766.2646

Toll Free 800.345.4669

FAX 304.558.6004

<https://brim.wv.gov/Pages/default.aspx>

- Ashley Summitt, Chief Privacy Officer – Ashley.E.Summitt@wv.gov, 304.352.0232
- Lori Tarr, Assistant Chief Privacy Officer – Lori.L.Tarr@wv.gov, 304.352.0251
- Tara Taylor, Administrative Assistant – Tara.L.Taylor@wv.gov, 304.352.0252