

Privacy and Cybersecurity A Partnership with Purchasing



State Privacy Office
WV Board of Risk and Insurance Management

September 19-20, 2019
2019 WV Agency Purchasing Conference

Objectives

- Learn about the West Virginia's State Privacy Program and Executive Branch Privacy Policies
- Learn about the importance of data privacy and the laws we must follow
- Raise awareness of the risks to data privacy
- Learn how we manage and reduce risk through our purchasing process and contracts
- Gain a better understanding of your role as a gatekeeper for protecting the State's data
- Learn about the Privacy Impact Assessment for technology and information systems

The world today is increasingly complex.



Creative Commons Complexity Wordle by versionz is licensed under CC BY 2.0

The need for managing risks to our privacy

RISK
MANAGEMENT



Increasing

Nick Youngson - <http://www.nyphotographic.com/>
Alpha Stock Images - <http://alphastockimages.com/>
<http://creativecommons-images.com/handwriting/r/risk-management.html>

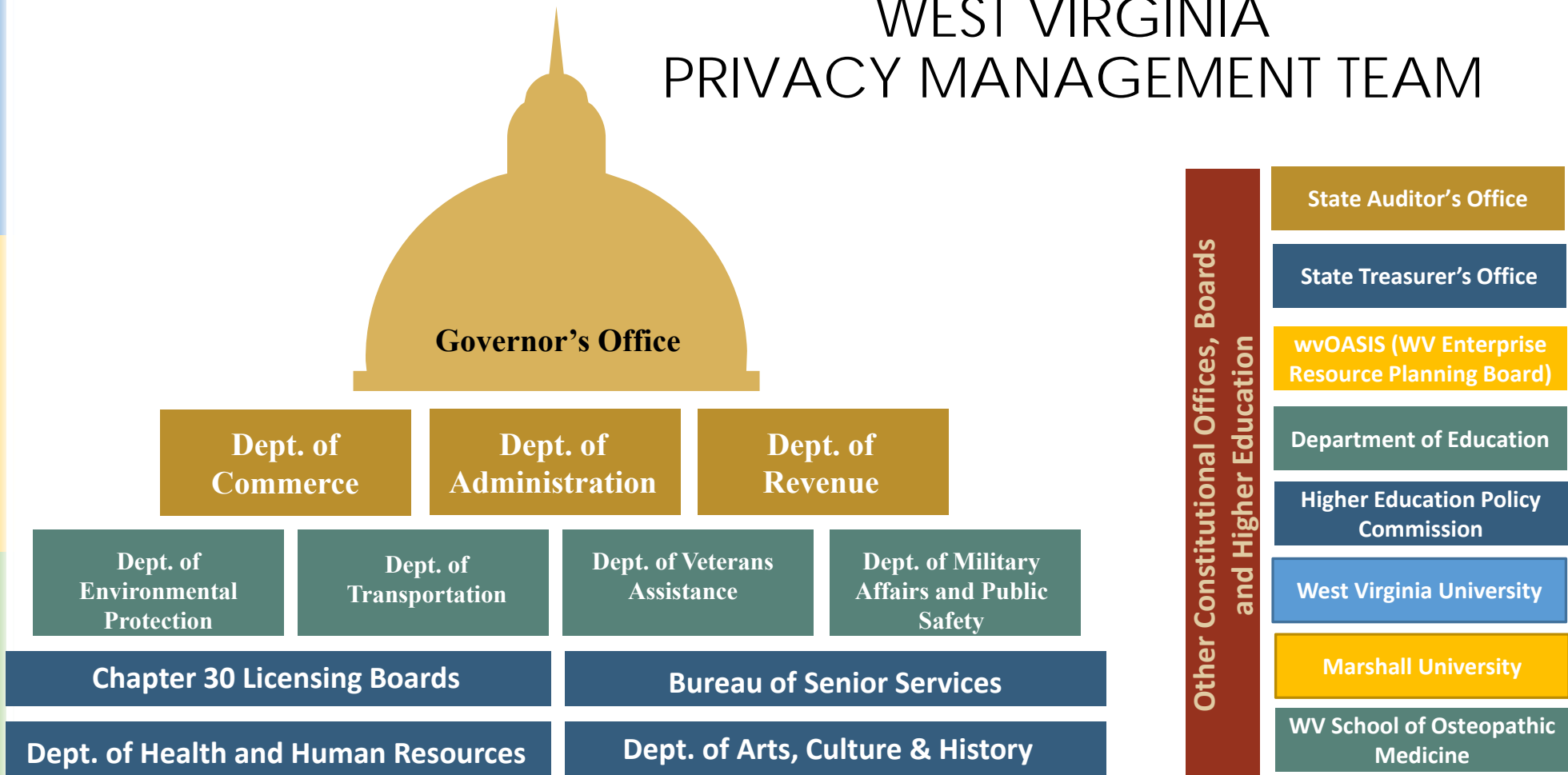


- Executive Order No. 3-17
- State Privacy Office, WV Board of Risk & Insurance Management
- Privacy Management Team
- Privacy Policies

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 18 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
- Sue Haga, Administrative Secretary
 - Oversees the privacy training done online through the LMS
 - Assists in incident response
 - Couldn't do-it-with-out-her person

WEST VIRGINIA PRIVACY MANAGEMENT TEAM



Privacy Policies

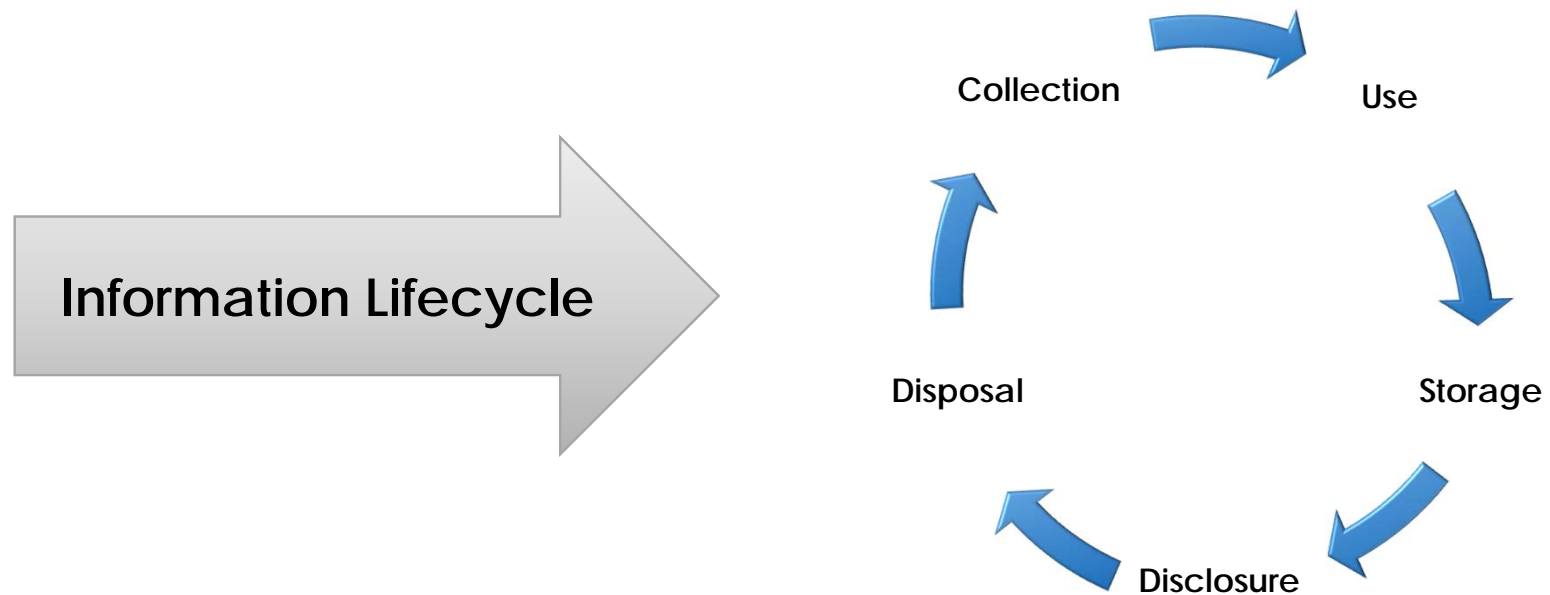
- The Privacy Program is based upon these six **Privacy Policies** consistent with law and regulation.
- Compliance is required for all Executive Branch Departments.



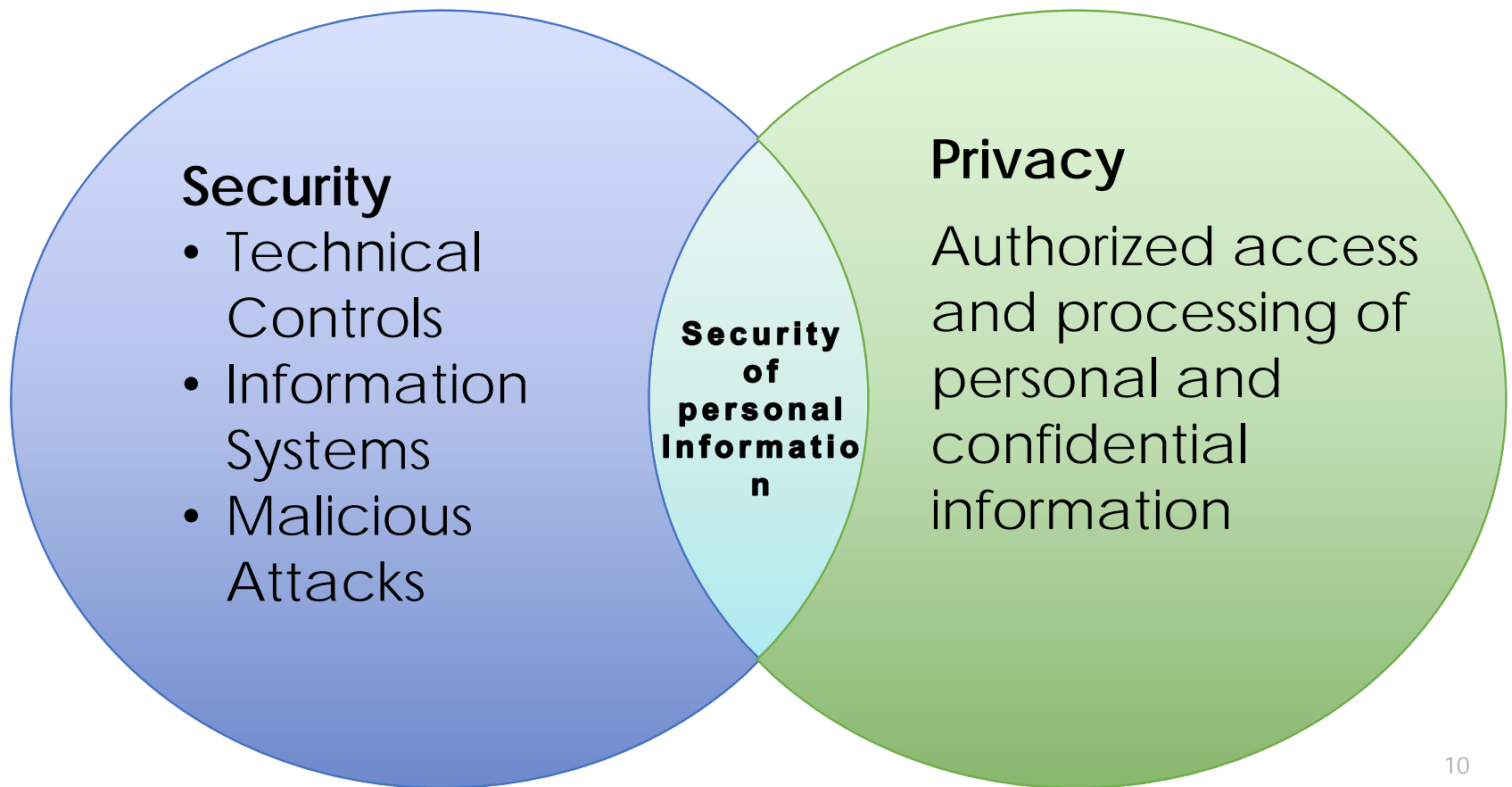
What is privacy?

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



Data Security and Data Privacy



Privacy's focus is about

Governance

- Policies
- Privacy Personnel
- Strategic Planning

Risk Management

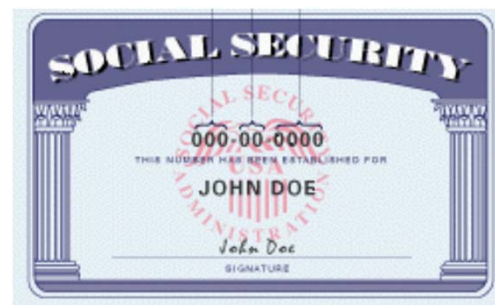
- Pro-active steps
- Training
- Privacy Impact Assessments

Incident Management

- Reporting
- Investigating
- Mitigating
- Compliance with notification requirements

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.



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?



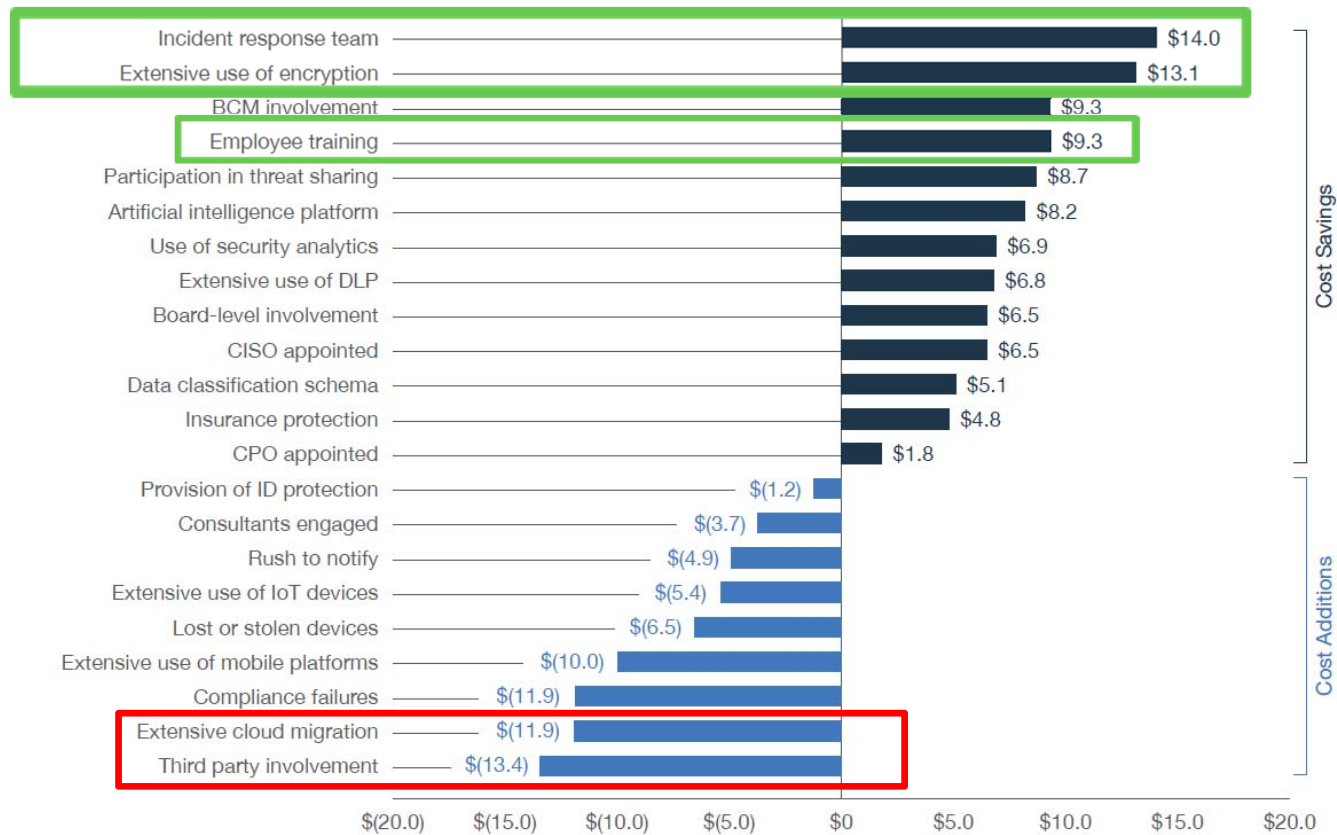
- **Data and security breaches are expensive**
- Civil and criminal penalties, including personal liability for criminal privacy violations
- U.S. - 2018 Cost per breached record: \$233
- Impact on costs per record*:
 - Third party (vendors) involvement - \$13 increase
 - Extensive cloud migration (at time of breach) - \$12 increase

Sources: Ponemon Institute, 2018 Global Cost of Data Breach Study
*Global costs

Factors that impact the per capita cost of a breach

Figure 12. Impact of 22 factors on the per capita cost of data breach

Measured in US\$



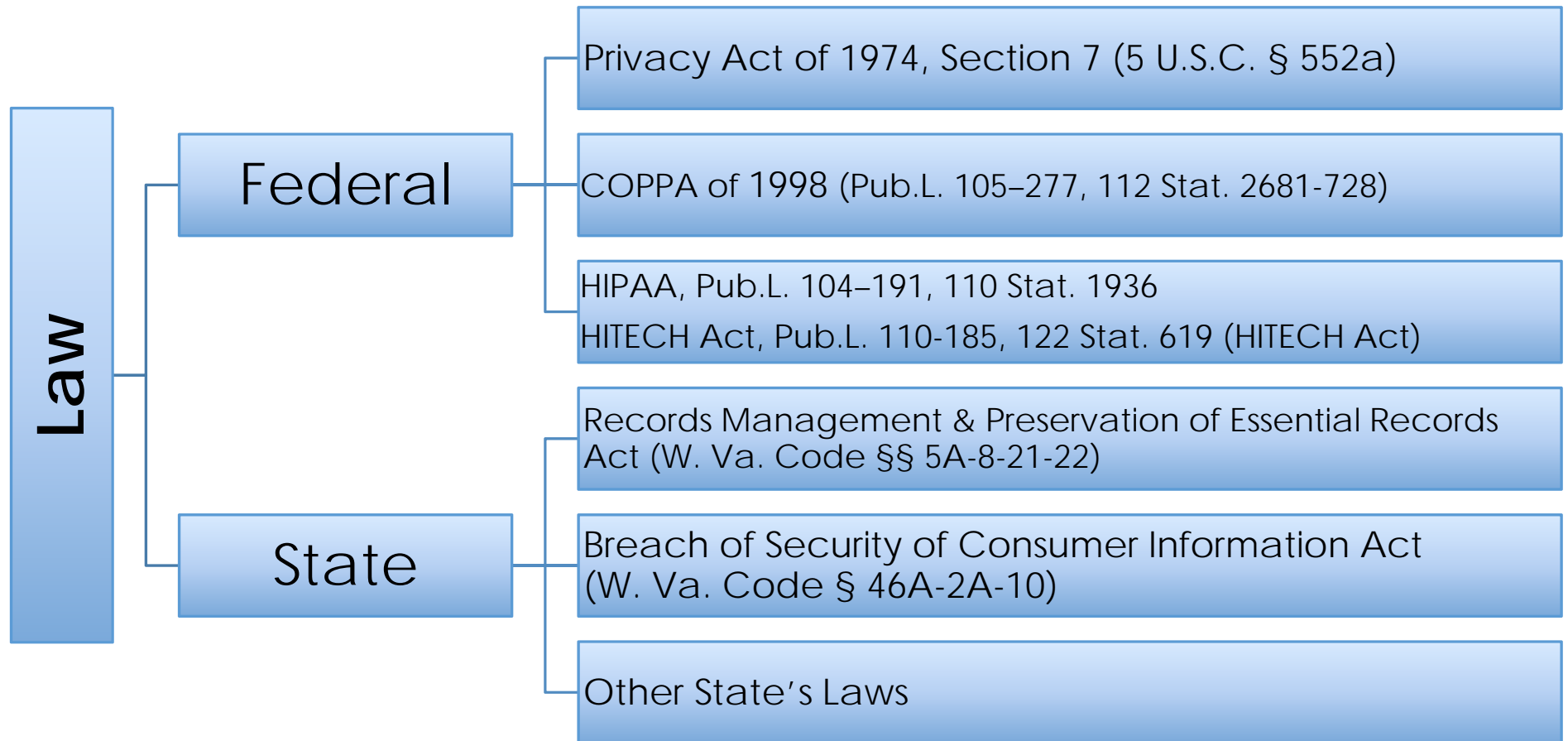
The Good News



- Impact on costs per record*:
 - Incident response teams - \$14 decrease
 - Extensive Encryption - \$13 decrease
 - Employee training - \$9 decrease

Sources: Ponemon Institute, 2018 Global Cost of Data Breach Study
*Global costs

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.

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 Act

- HIPAA (Health Insurance Portability and Accountability Act of 1996)
 - HIPAA Privacy Rule
 - HIPAA Security Rule
- 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

HIPAA Protects PHI

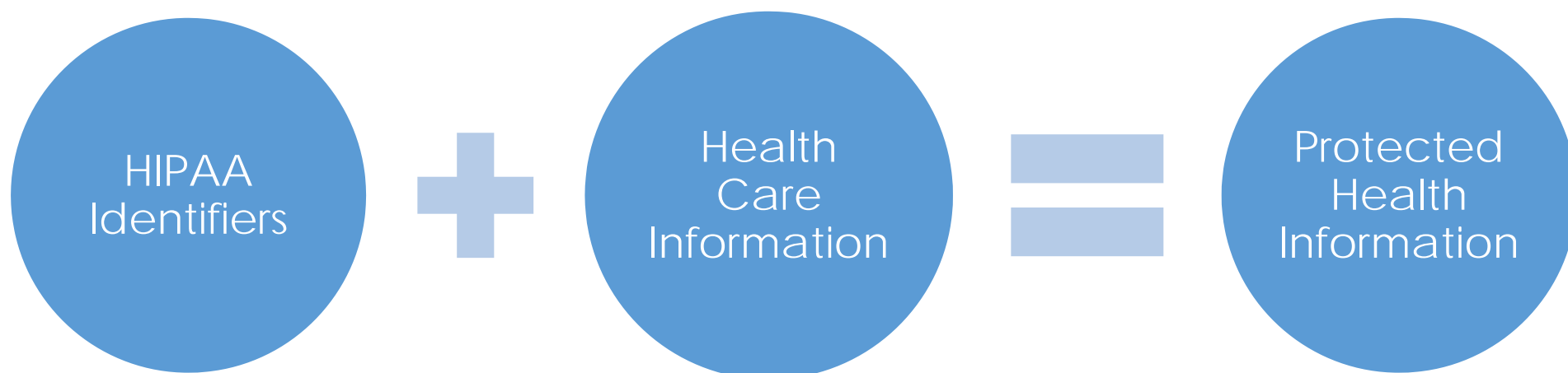
- In any form or media – electronic, paper or oral
- Relates to an individual's:
 - Physical or mental condition
 - Provision of health care to the individual, or
 - Payment for the provision of health care
 - Past, present or future

HIPAA Identifiers

- Patient names
- Geographic subdivisions (smaller than state)
- Telephone numbers
- Fax numbers
- Social Security numbers
- Vehicle identifiers
- E-mail addresses
- Web URLs and IP addresses
- Dates (except year)
- Names of relatives, employers and household members
- Full face photographs or images
- Medical record numbers
- Account numbers
- Biometric identifiers (fingerprints or voiceprints)
- Device identifiers
- Health plan beneficiary numbers
- Certificate/license numbers
- Any other unique number, code, or characteristic that can be linked to an individual.

Not all health information is PHI

- Covered Entities
- Business Associates



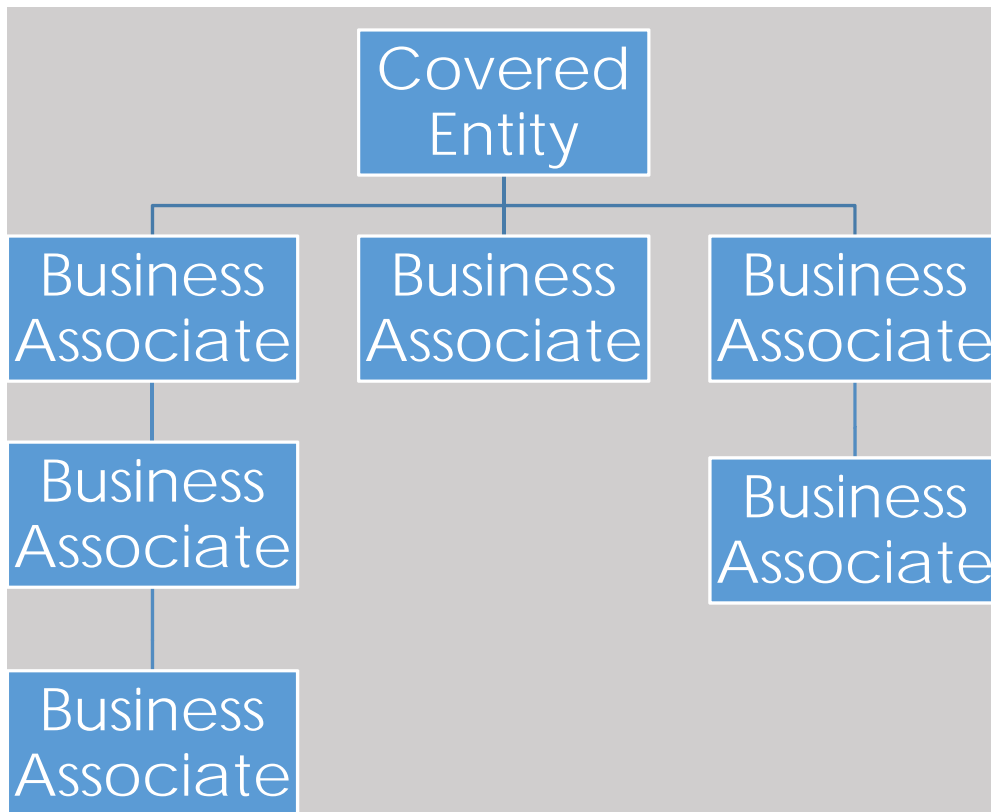
Federal HITECH Act

- HITECH Act (Health Information Technology for Economic and Clinical Health Act of 2009) –
 - Strengthened HIPAA with breach notification rule for unauthorized disclosures, except when a risk analysis could demonstrate a low risk of compromise.
 - Included civil penalties and criminal enforcement.
 - Further promoted the adoption of health information technology and set standards for meaningful use of Electronic Health Records (EHRs).

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 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

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

OCR Enforcement - Civil Monetary Penalties

HIPAA Violation	Minimum Penalty	Maximum Penalty
Unknowing	\$100 per violation, with an annual maximum of \$25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation)	\$50,000 per violation, with an annual maximum of \$1.5 million
Reasonable Cause	\$1,000 per violation, with an annual maximum of \$100,000 for repeat violations	\$50,000 per violation, with an annual maximum of \$1.5 million
Willful neglect but violation is corrected within the required time period	\$10,000 per violation, with an annual maximum of \$250,000 for repeat violations	\$50,000 per violation, with an annual maximum of \$1.5 million
Willful neglect and is not corrected within required time period	\$50,000 per violation, with an annual maximum of \$1.5 million	\$50,000 per violation, with an annual maximum of \$1.5 million

<https://www.ama-assn.org/practice-management/hipaa-violations-enforcement>

HIPAA Enforcer: Department of Health and Human Services' Office for Civil Rights (OCR)



OCR's most frequent target areas for non-compliance investigations

<https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html>

Impermissible uses and disclosures of protected health information (PHI)

Lack of safeguards of PHI

Lack of patient access to their PHI

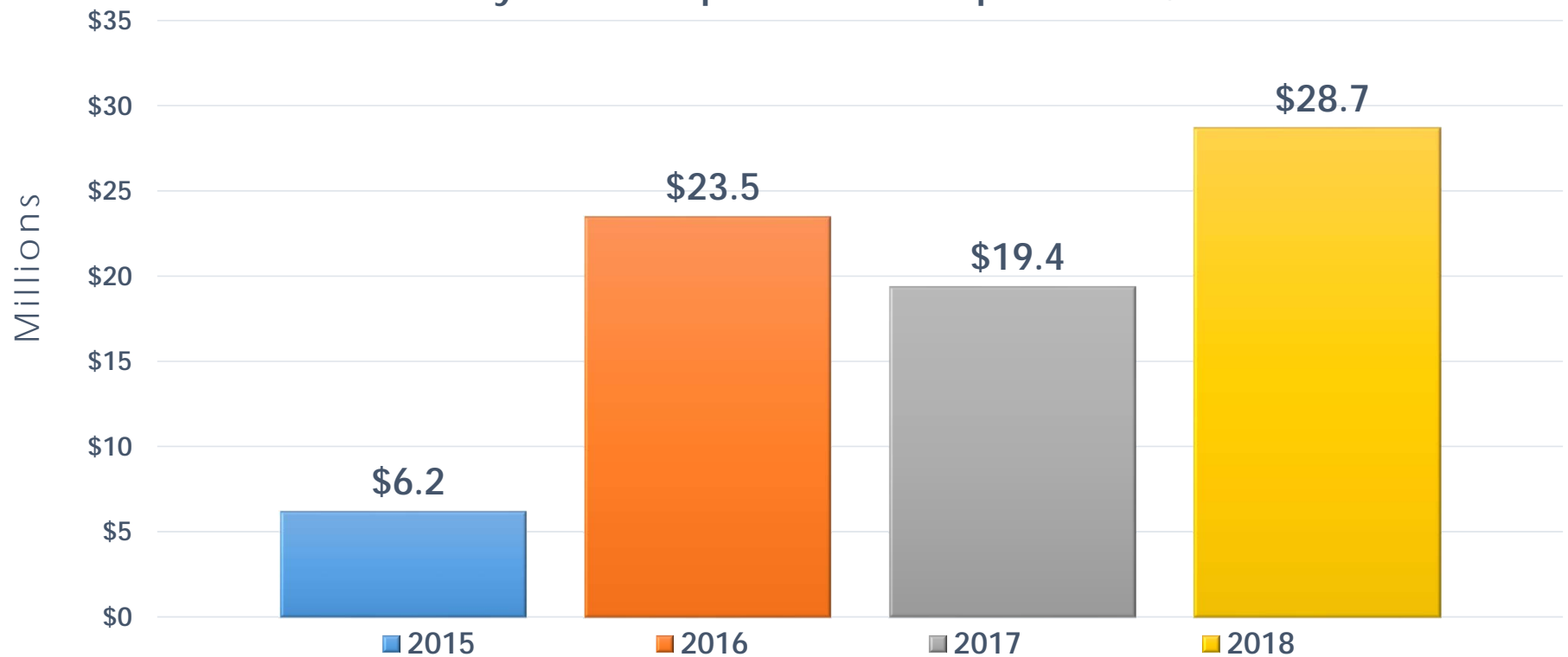
Lack of administrative safeguards of ePHI

Use or disclosure of more than the minimum necessary PHI

OCR Settlements and Judgements: 2015 – 2018

(In Millions)

Total since Privacy Rule compliance date April 2003: \$96.6 million



Sources:

- <https://www.hipaajournal.com/a-year-of-hipaa-enforcement-ocr-hipaa-penalties-issued-in-2015-8258/>
- <https://www.hipaajournal.com/ocr-hipaa-enforcement-summary-2016-hipaa-settlements-8646/>
- <https://www.hipaajournal.com/2017-hipaa-enforcement-summary/>
- <https://www.hhs.gov/sites/default/files/2018-ocr-hipaa-summary.pdf>

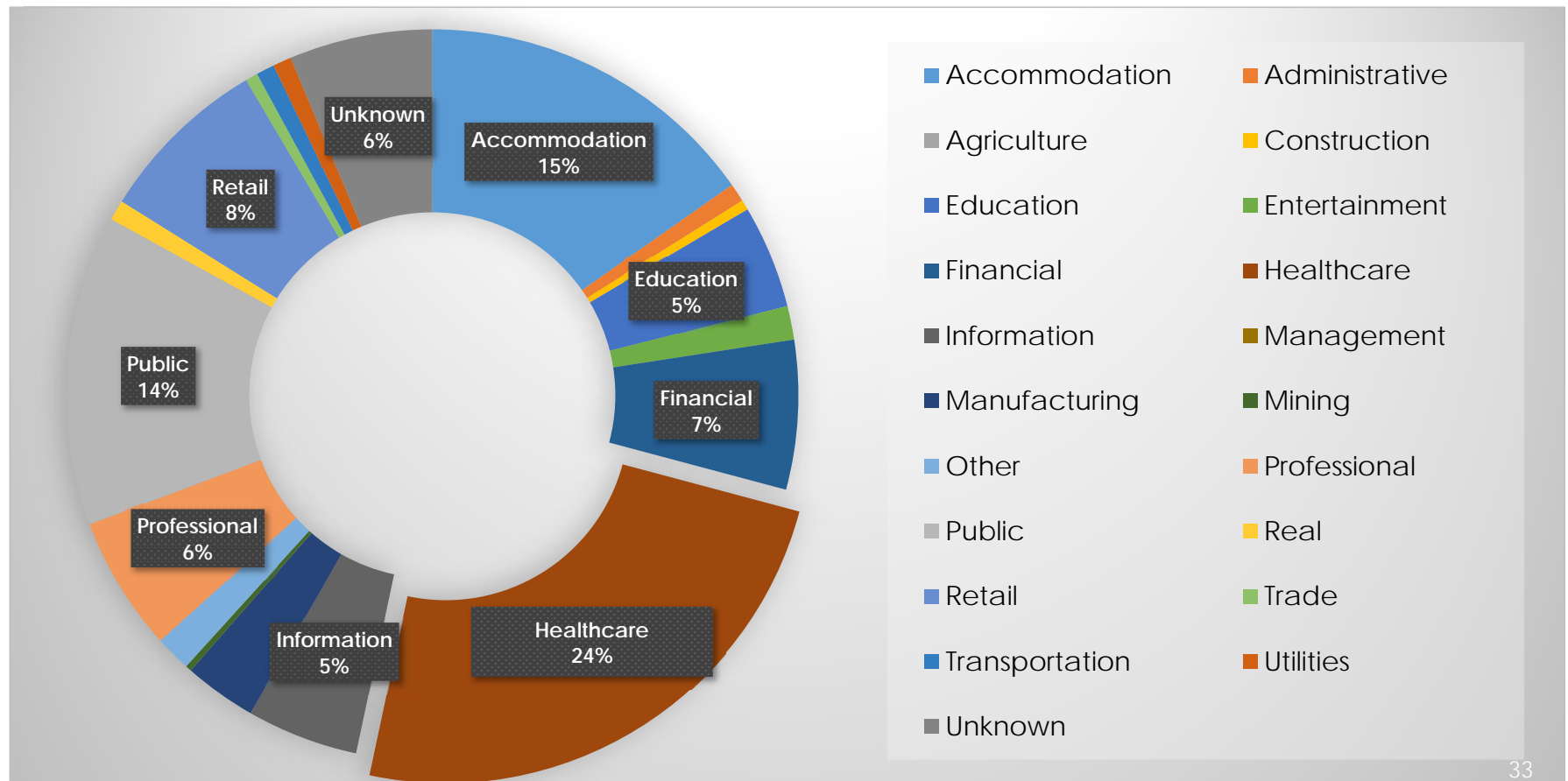
Criminal Penalties - DOJ

1. Offenses where the organization or individual "knowingly" obtained or disclosed individually identifiable health information, in violation of HIPAA, are subject to a fine of up to \$50,000, as well as imprisonment up to 1 year
2. Offenses committed under false pretenses could be prosecuted with a \$100,000 fine, with up to 5 years in prison
3. Offenses committed with the intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain or malicious harm may result fines of \$250,000 and imprisonment up to 10 years

Breaches by Industry Sector – Percentage

Source: Verizon 2018 Data Breach Investigations Report

Data: 11.1.16 - 10.31.17



Insider Threats

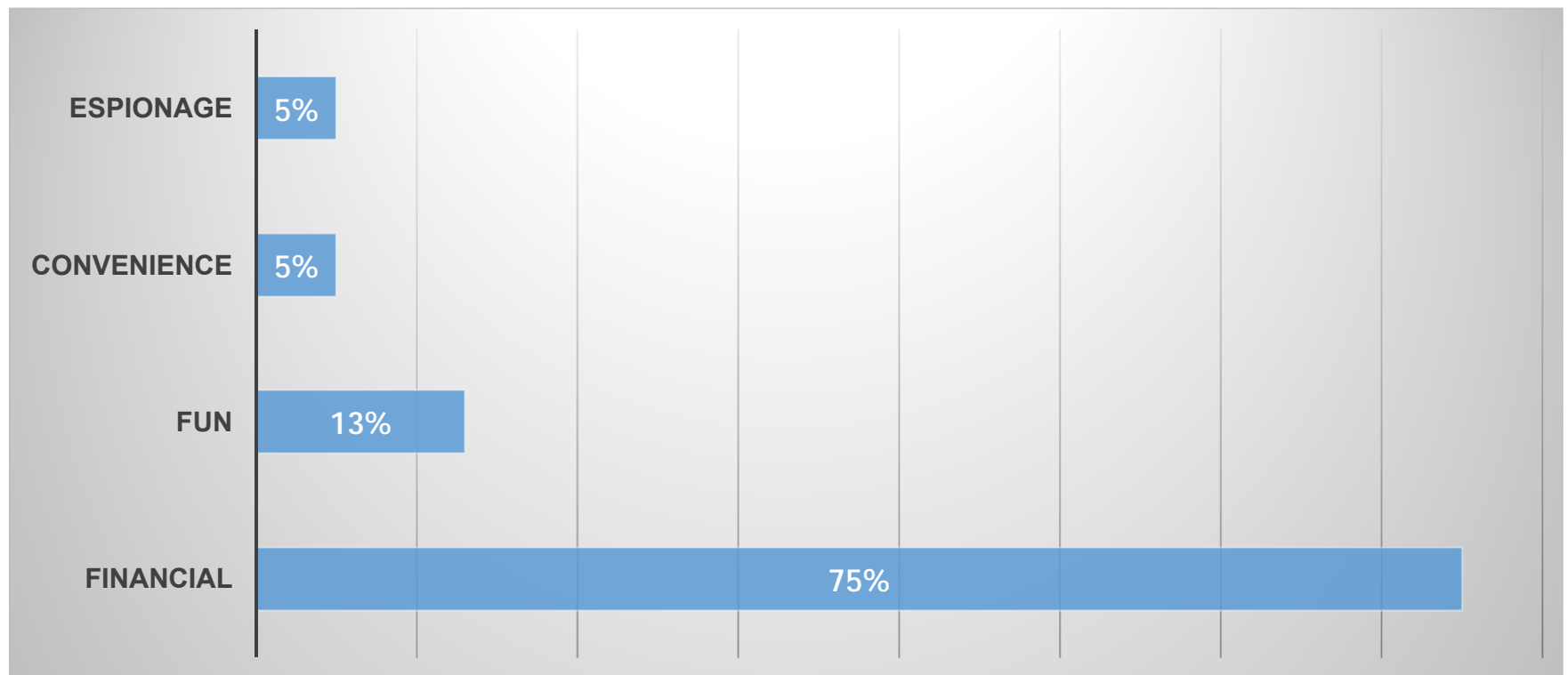
Healthcare is identified as the only industry that has the greatest breach threat from its workforce.

- Errors
- Misuse
 - Curiosity
 - Financial gain

Source: Verizon's 2018 Data Breach Investigation Report

Bad Actor Motives – Healthcare Incidents

Source: Verizon 2018 Data Breach Investigations Report
Data: 11.1.16 - 10.31.17



Healthcare Data More Valuable than Financial Data

“Healthcare records are more valuable to attackers and sell for significantly higher than financial data on the dark web...

- Stolen healthcare information can be used to
 - file false claims with insurance carriers or
 - create false IDs to purchase drugs.
- And unlike credit card numbers, which are cancelled relatively quickly once identified as compromised, healthcare information can be used for nefarious purposes over longer periods of time.”

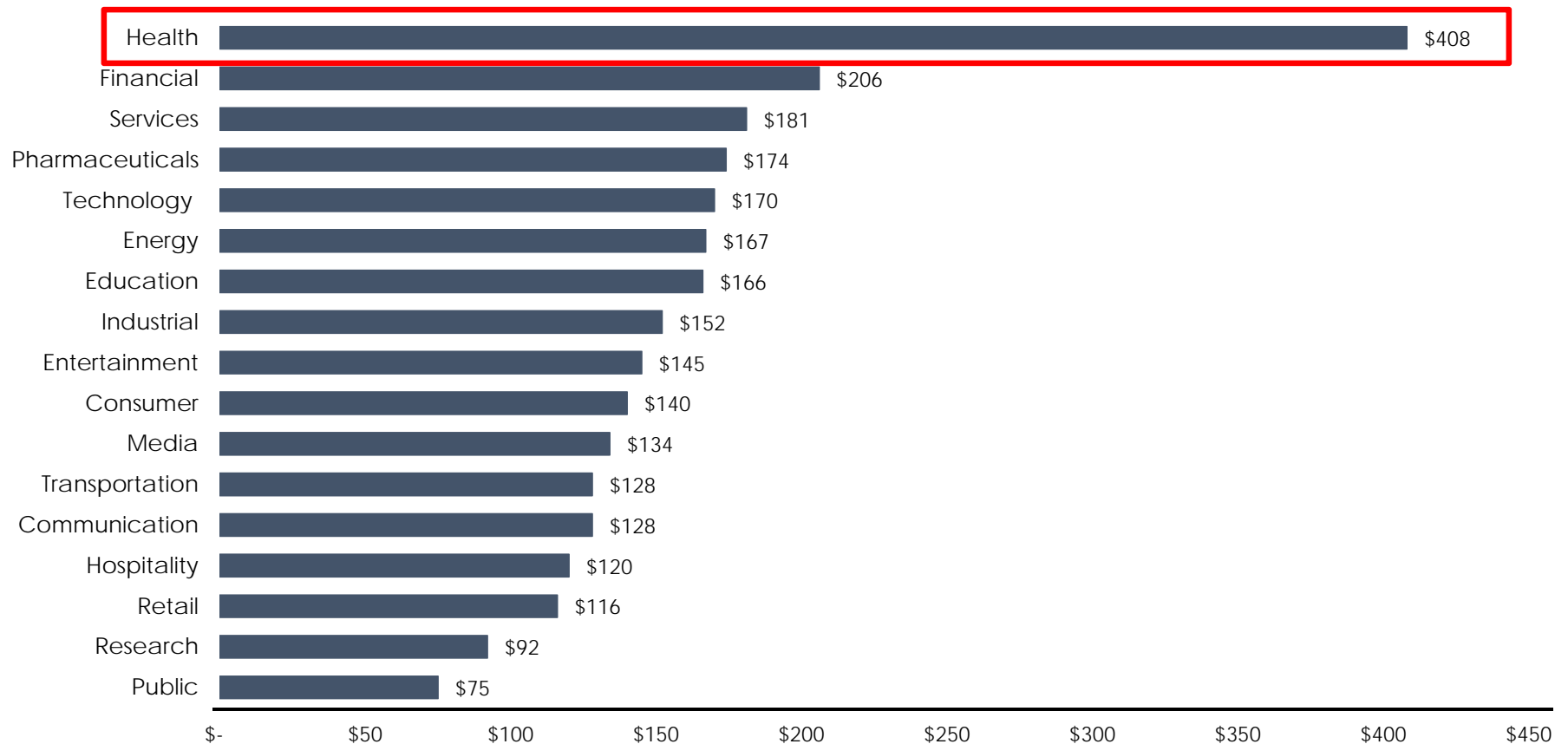
Beazley Privacy Breach Response Services Manager, Lauren Winchester

Source: <https://www.crowdfundinsider.com/2019/04/145971-insurer-beazley-healthcare-industry-most-targeted-by-cyber-attacks/>

Per capita Cost by Industry Sector: Healthcare the Most Expensive

Source: Ponemon 2018 Cost of a Data Breach Report

Data: Majority of data occurred within 2017



Root Cause of Data Breaches

Source: Ponemon 2018 Cost of a Data Breach Report

Data: Majority of data occurred within 2017

27%

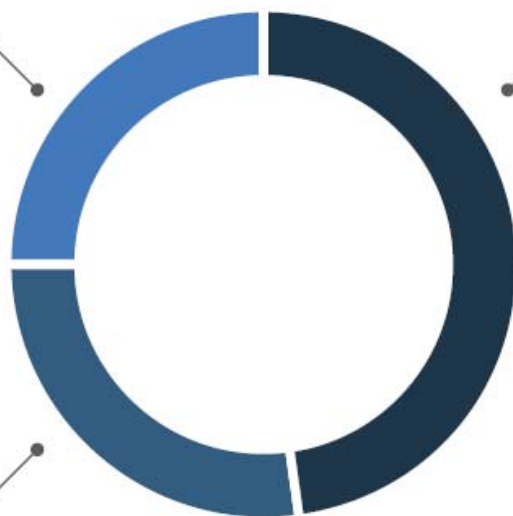
Human error

System glitch

25%

48%

Malicious or
criminal attack



General Terms and Conditions includes

- Privacy, Security, and Confidentiality term #30:
 - Purchasing Division Review
 - Confidentiality from vendor workforce
 - Vendor compliance with confidentiality and security requirements
 - Link to Purchasing's Privacy and Confidentiality Webpage

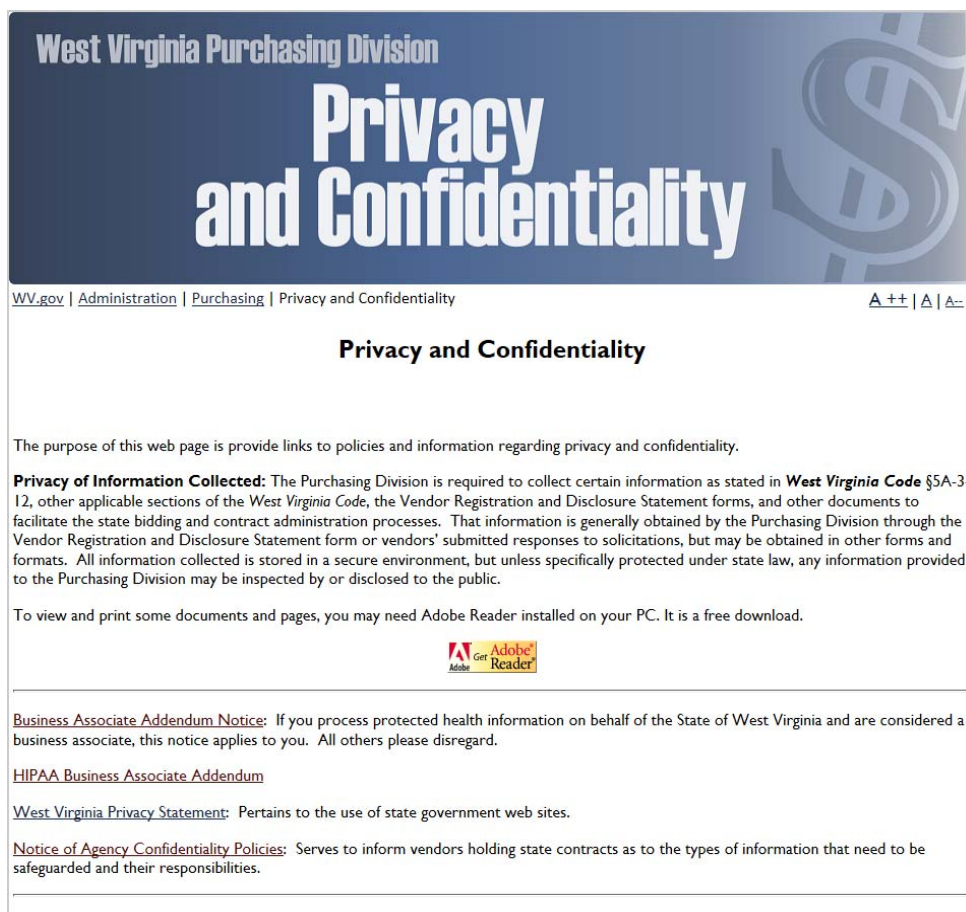
30. PRIVACY, SECURITY, AND CONFIDENTIALITY: The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the Agency, unless the individual who is the subject of the information consents to the 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>.

General Terms and Conditions includes

- Privacy, Security, and Confidentiality term #29:
 - Agency Delegate Procurements
 - Confidentiality from vendor workforce
 - Vendor compliance with confidentiality and security requirements
 - Link to Purchasing's Privacy and Confidentiality Webpage

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>

Privacy and Confidentiality Webpage



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

Order of Precedent and Modification Addendum

NOW THEREFORE, the Parties hereto hereby agree as follows:

1. **Order of Precedence:** The Contract is comprised of the documents listed in this section. The terms and conditions contained in the various documents shall be interpreted according to the priority given to the Contract document in this section. In that way, any terms and conditions contained in the first priority document shall prevail over conflicting terms in the second priority document, and so on.

Contract Documents:

- a. **Order of Precedence and Modification Addendum** (this document) – First Priority
 - b. **WV-96 Agreement Addendum** (Attached as Exhibit A) – Second Priority
 - c. **General Terms and Conditions** (Attached as Exhibit B)– Third Priority
 - d. **Notice of State of West Virginia Confidentiality Policies and Information Security Accountability Requirements** (Attached as Exhibit C)
 - e. **Vendor** (Attached as part of Exhibit D)– Fourth Priority
 - f. **Redacted** Security Practices (Attached as part of Exhibit D) – Fifth Priority
- 

HIPAA/HITECH – Departments/Programs

- Components of - covered entities, business associates
 - Department of Administration
 - PEIA – Covered Entity
 - OT – Business Associate for PEIA, DHHR
 - Department of Health and Human Resources
 - Department of Veteran's Assistance
 - Bureau of Senior Services
- Contact your Department Privacy Officer to determine coverage
 - <https://privacy.wv.gov/about/Pages/default.aspx>

Vendor Resource Center

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

OR

Privacy and Confidentiality Webpage

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>.

WV HIPAA Business Associate Addendum

- **Definitions**
- **Permitted Uses and Disclosures**
 - PHI Described
 - Purposes
 - Further Uses and Disclosures
- **Obligations of BAs**
 - Stated Purposes Only
 - Limited Disclosure
 - Prohibits BA from marketing activities that would violate HIPAA
 - Safeguards
 - Comply with Security Standards for ePHI
 - Safeguard all PHI
- Mitigation
- Compliance with law
- Support of Individual Rights
- Notification of Breach
 - Report to State
 - Costs borne by BA
 - Downstream subcontracting to contain same requirements
- Assistance in Litigation or Administrative Proceedings
- **Addendum Administration**
 - Termination of contract
- **General Provisions/Ownership of PHI**

Procurement Officers are 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)

Minimum Necessary Principle – Don't let your agency cause a breach!

Review for PII

- Home addresses
- Social Security number
- Birth date
- Birth, adoption or death certificate
- Credit/Debit Card Number
- Financial records (Loan Accounts, Payment History, Consumer Reports)
- Check/Savings/Other Financial Account Numbers
- Mother's maiden name and marital status
- Biometric identifiers
- Driver ID Number or State ID number issued in lieu thereof
- Criminal records & history
- Medical, Disability or Employment Records

The path forward . . .

- 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.
- Require your Department Privacy Officer to complete or have completed a Privacy Impact Assessment (PIA) which will let you know whether PII is involved or a BAA is required.
- Keep a copy of the PIA for your file.

What is a Privacy Impact Assessment?

A Privacy Impact Assessment, or PIA, is a systematic analysis that addresses:

- Privacy issues intrinsic to an information system, or process, that involves Personally Identifiable Information (PII) or other confidential information
- The consequences for privacy throughout the life-cycle of the data – collection, use, storage, disclosure and destruction.
- Risks associated with the project or process
- Mitigation of risk through the use of privacy and security controls
- Compliance with legal, regulatory, and policy requirements

When should a PIA be completed?

Useful as a privacy management tool to evaluate the implications of



New
Information
Systems

New
Technology
Purchases

Significantly
Modified
Information
Systems

Project Timing

Project Initiation

Design phase

Prior to implementation

Completed projects or processes

Privacy Impact Assessment

- Current format:
 - Excel Workbook

Worksheet 1
General Information

West Virginia Executive Branch Privacy Impact Assessment

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



PIA Components – Cloud Vendor Highlights

- Section 5 – Data Disclosure
 - Question 20 identifies which vendor agreements are required
 - It includes the SaaS Addendum for host applications in the cloud that are accessed via the internet

20. If your project involves a vendor, which agreements are needed? (Check all that apply.)	
<input type="checkbox"/>	Memorandum of Understanding
<input type="checkbox"/>	Vendor Contract
<input type="checkbox"/>	Privacy, Security and Confidentiality Contract Term ¹
<input type="checkbox"/>	Business Associate Addendum ²
<input type="checkbox"/>	Software as a Service Addendum ³
<input type="checkbox"/>	Other
<input type="checkbox"/>	N/A

¹ For use when the vendor will process your Personally Identifiable Information (PII). This term is located in Agency and Purchasing Master Terms and Conditions.

² For use when your agency is a HIPAA covered entity, or business associate, and the vendor will process your Protected Health Information (PHI).

³ For use when the vendor will host applications in the cloud that are accessed using the internet.

Resources

- To report an incident or breach, go to the OT portal:
<https://apps.wv.gov/ot/ir/Default.aspx>
- If you don't know who your privacy officer is, you can find the name here: <https://privacy.wv.gov/about/Pages/default.aspx>
- Work with privacy officer, to determine whether a Business Associate Addendum (BAA) is needed
 - Determine whether the vendor is processing PHI under contract. If yes,
 - Make sure a PIA is completed. Follow guidance from a Privacy Impact Assessment (PIA). If a PIA has not been completed, send the Project Manager and/or Department Privacy Officer this link:
<http://www.privacy.wv.gov/privacyimpactassessment/Pages/default.aspx>
- To determine whether a contract term to protect privacy, security and confidentiality is needed, review the PIA.

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>

Questions? And...

...Don't forget to sign the attendance sheet.



Contact Information

- Ashley Summitt, Chief Privacy Officer – Ext. 57624 – ashley.e.summitt@wv.gov
- Lori Tarr, Assistant Chief Privacy Officer – Ext. 57616- lori.l.tarr@wv.gov
- Sue Haga, Administrative Secretary (Privacy Office) – Ext. 57626 – sue.c.haga@wv.gov

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