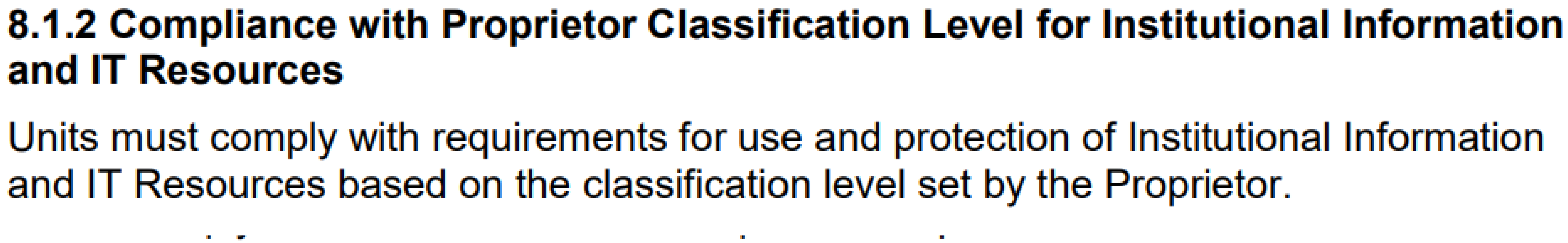
UC Davis Data Classification Research Focus

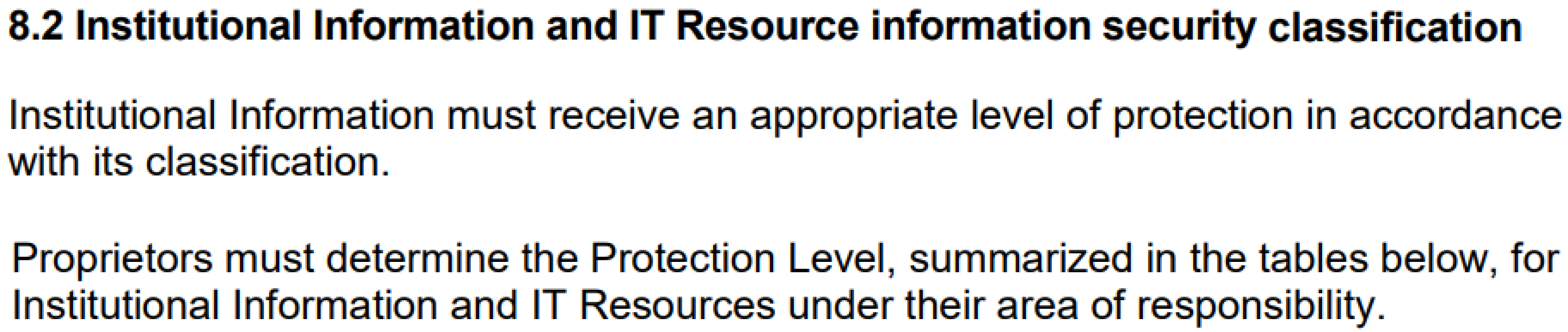
2024

IS-3 Policy



8.1.2 Compliance with Proprietor Classification Level for Institutional Information and IT Resources

Units must comply with requirements for use and protection of Institutional Information and IT Resources based on the classification level set by the Proprietor.



8.2 Institutional Information and IT Resource information security classification

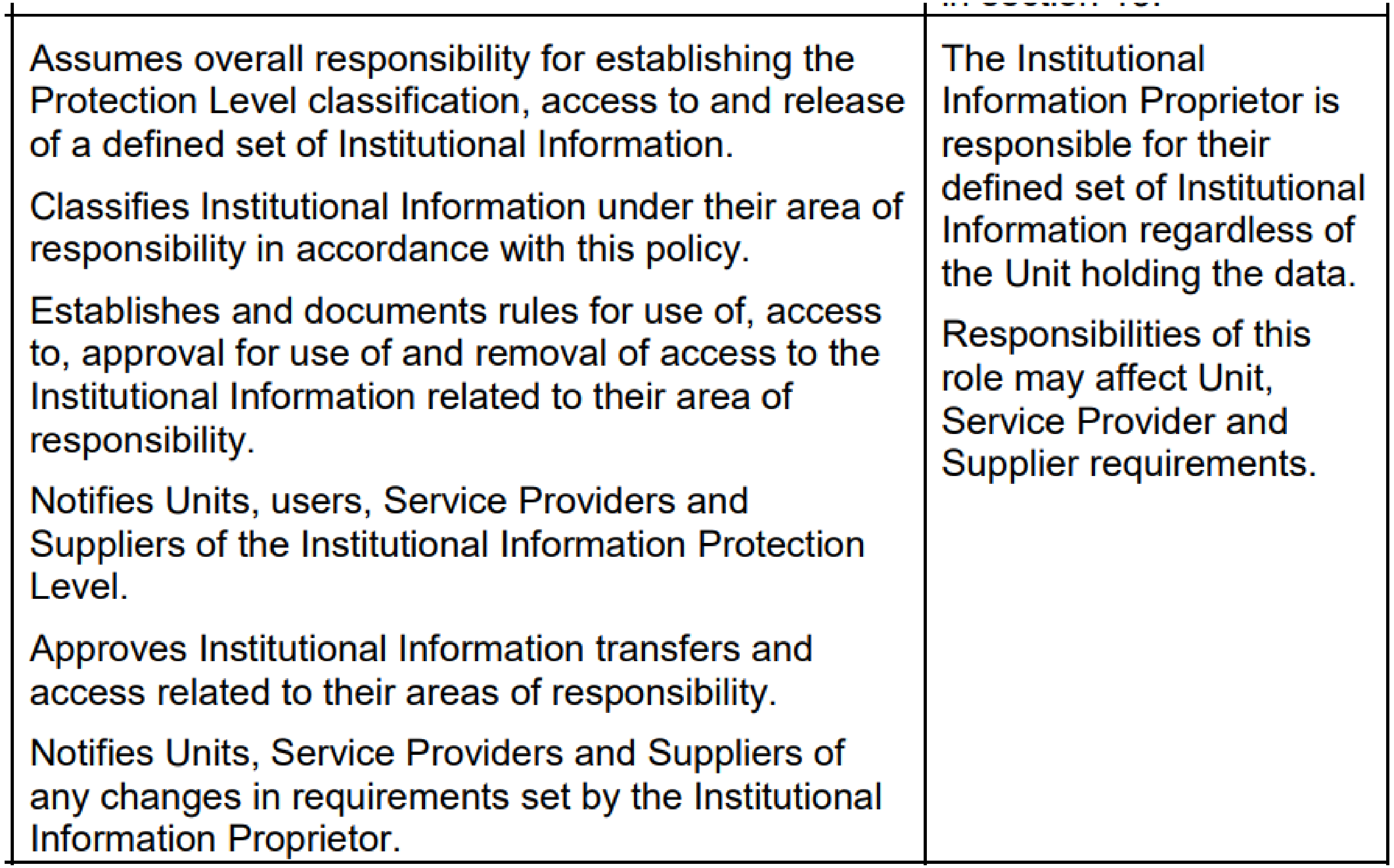
Institutional Information must receive an appropriate level of protection in accordance with its classification.

Proprietors must determine the Protection Level, summarized in the tables below, for Institutional Information and IT Resources under their area of responsibility.

https://policy.ucop.edu/doc/7000543/BFB-IS-3

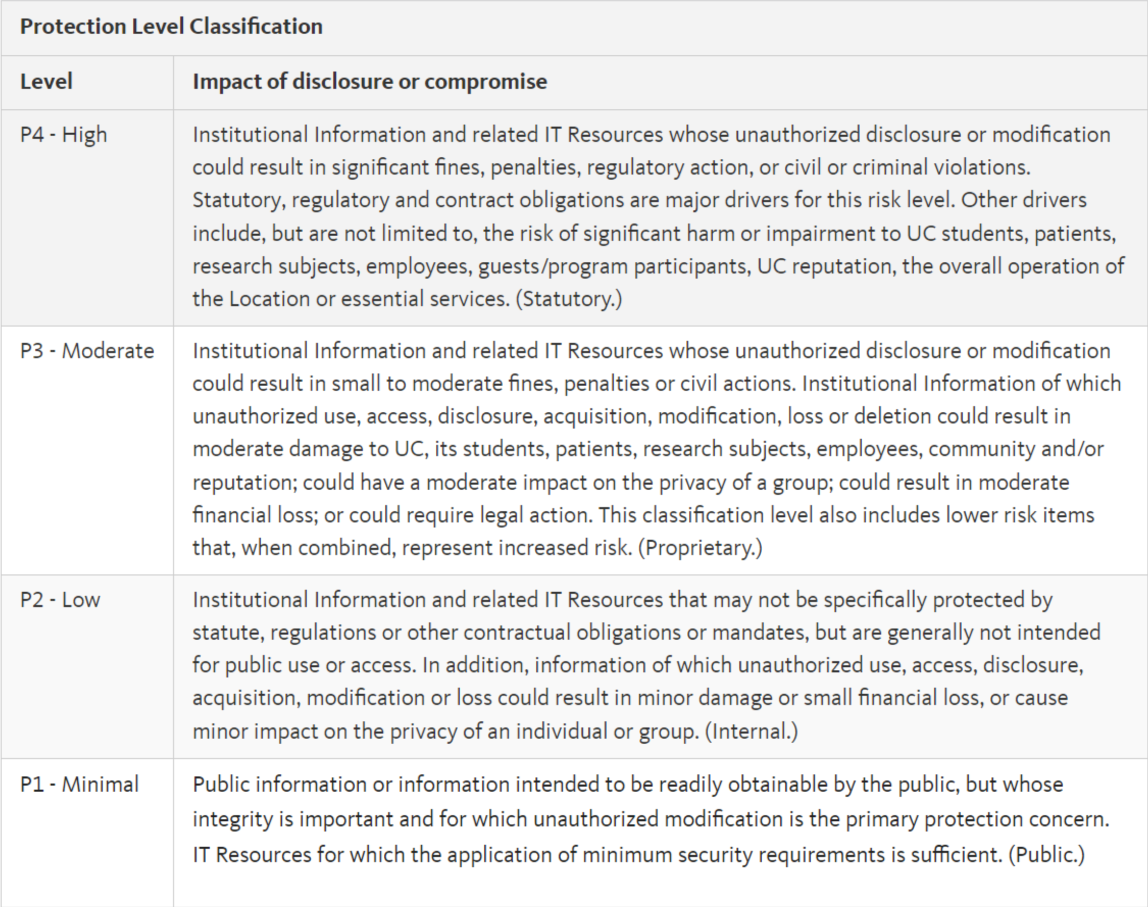
Proprietor

- Overall responsibility
- Data classification
- Documentation
- Notification
- Transfer approval



Assumes overall responsibility for establishing the Protection Level classification, access to and release of a defined set of Institutional Information. Classifies Institutional Information under their area of responsibility in accordance with this policy. Establishes and documents rules for use of, access to, approval for use of and removal of access to the Institutional Information related to their area of responsibility. Notifies Units, users, Service Providers and Suppliers of the Institutional Information Protection Level. Approves Institutional Information transfers and access related to their areas of responsibility. Notifies Units, Service Providers and Suppliers of any changes in requirements set by the Institutional Information Proprietor.	The Institutional Information Proprietor is responsible for their defined set of Institutional Information regardless of the Unit holding the data. Responsibilities of this role may affect Unit, Service Provider and Supplier requirements.

UC Data Classification Guide and Standard



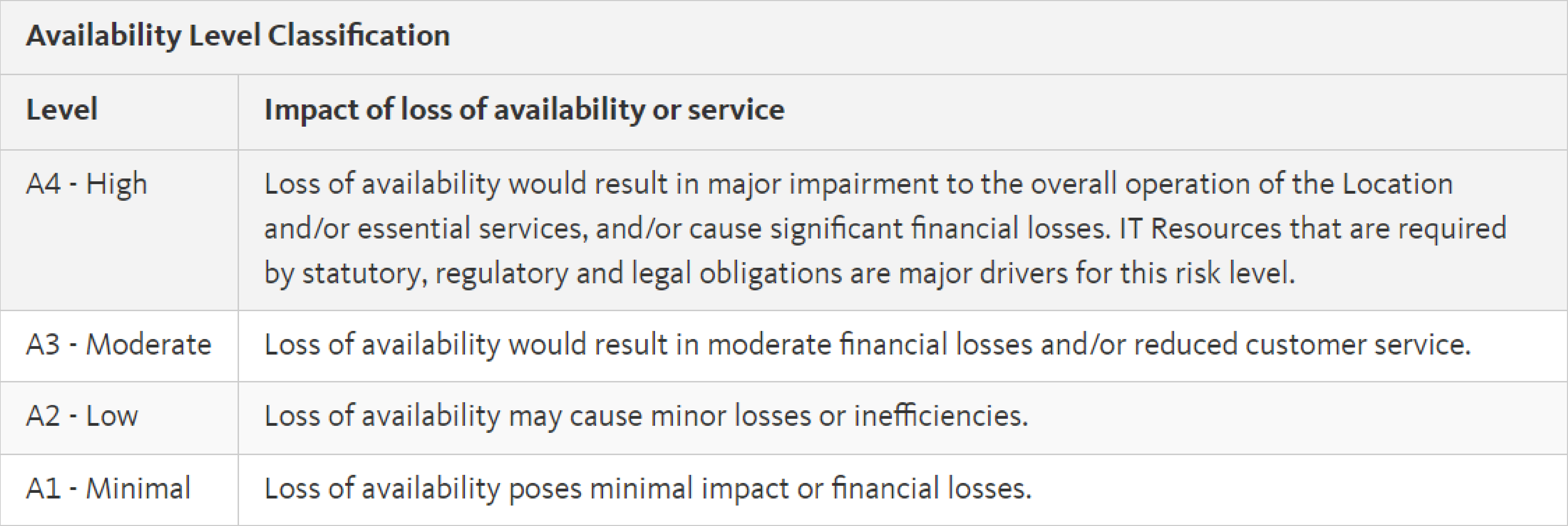
Protection Level Classification	
Level	**Impact of disclosure or compromise**
P4 - High	Institutional Information and related IT Resources whose unauthorized disclosure or modification could result in significant fines, penalties, regulatory action, or civil or criminal violations. Statutory, regulatory and contract obligations are major drivers for this risk level. Other drivers include, but are not limited to, the risk of significant harm or impairment to UC students, patients, research subjects, employees, guests/program participants, UC reputation, the overall operation of the Location or essential services. (Statutory.)
P3 - Moderate	Institutional Information and related IT Resources whose unauthorized disclosure or modification could result in small to moderate fines, penalties or civil actions. Institutional Information of which unauthorized use, access, disclosure, acquisition, modification, loss or deletion could result in moderate damage to UC, its students, patients, research subjects, employees, community and/or reputation; could have a moderate impact on the privacy of a group; could result in moderate financial loss; or could require legal action. This classification level also includes lower risk items that, when combined, represent increased risk. (Proprietary.)
P2 - Low	Institutional Information and related IT Resources that may not be specifically protected by statute, regulations or other contractual obligations or mandates, but are generally not intended for public use or access. In addition, information of which unauthorized use, access, disclosure, acquisition, modification or loss could result in minor damage or small financial loss, or cause minor impact on the privacy of an individual or group. (Internal.)
P1 - Minimal	Public information or information intended to be readily obtainable by the public, but whose integrity is important and for which unauthorized modification is the primary protection concern. IT Resources for which the application of minimum security requirements is sufficient. (Public.)

https://security.ucop.edu/policies/institutional-information-and-it-resource-classification.html

References to Research

- Researchers should be aware that health and medical information about research subjects may also be regulated by HIPAA, California Information Practices Act (IPA) or CMIA.
- P4 - Human subject research data with individual identifiers, particularly identifiers listed in law.
- P4 – as classified by IRB, stored in high security environment
- P3 – Animal research protocols
- Etc.

Availability Level Classification

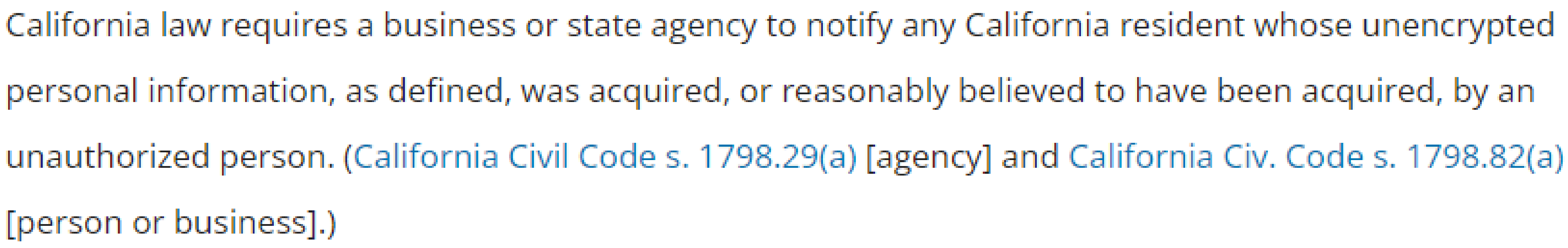


Availability Level Classification

Level	Impact of loss of availability or service
A4 - High	Loss of availability would result in major impairment to the overall operation of the Location and/or essential services, and/or cause significant financial losses. IT Resources that are required by statutory, regulatory and legal obligations are major drivers for this risk level.
A3 - Moderate	Loss of availability would result in moderate financial losses and/or reduced customer service.
A2 - Low	Loss of availability may cause minor losses or inefficiencies.
A1 - Minimal	Loss of availability poses minimal impact or financial losses.

Data Classification, but also IS-3, CCPA, CMIA, HIPAA, HITECH, GDPR

- CCPA – California Consumer Privacy Act
- CCPA Opt In Consent – For children under age 16 years
- PCI DSS – Payment Card Industry Data Security Standard
- CMIA – California Confidentiality of Medical Information Act
- HITECH – strengthened the privacy and security provisions of HIPAA
- GDPR – General Protection Regulation, imposes obligation anywhere
- And more



California law requires a business or state agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. (California Civil Code s. 1798.29(a) [agency] and California Civ. Code s. 1798.82(a) [person or business].)

Breach Notification and Encryption

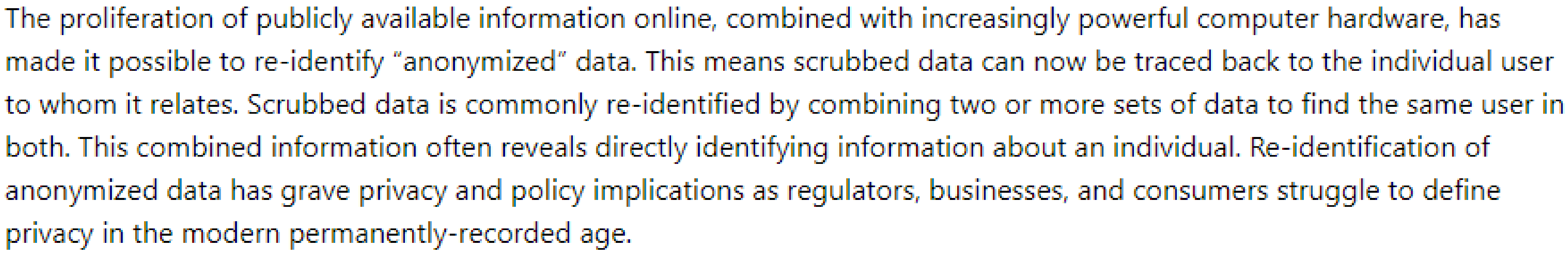
Funding or data sponsor requirements?

- Protection according to a specific standard?
- Attestation of compliance with a standard?
- What type of notification if protection fails?
- Impact of non-compliance?
  - Loss of future funding?
  - Fines?
  - Reputational damage?

Bottom line…………………………………………………………..this could be about more than just IS-3

Lessons Learned – Medical information

- P4 medical information
- P4 medical information subject to HIPAA
- CMIA requirements more stringent than HIPAA
- Special accommodation that does not disclose medical status
- FERPA vs. HIPAA
- Animal health records
  - Legal requirements
  - Impact of upset owner?



The proliferation of publicly available information online, combined with increasingly powerful computer hardware, has made it possible to re-identify "anonymized" data. This means scrubbed data can now be traced back to the individual user to whom it relates. Scrubbed data is commonly re-identified by combining two or more sets of data to find the same user in both. This combined information often reveals directly identifying information about an individual. Re-identification of anonymized data has grave privacy and policy implications as regulators, businesses, and consumers struggle to define privacy in the modern permanently-recorded age.

RE-Identification of "Anonymized" Data
Georgetown Law Technology Review
Boris Lubarsky, April 2017

Question

We have a de-identified data set that we need to upload into coldstoorage.com

Do we need to do a Vendor Risk Assessment of coldstoorage.com?

Types of Data

PSEUDONYMOUS

Information from which direct identifiers have been eliminated or transformed, but indirect identifiers remain intact

DE-IDENTIFIED

Direct and known indirect identifiers have been removed or manipulated to break the linkage to real world identities

ANONYMOUS

Direct and indirect identifiers have been removed or manipulated together with mathematical and technical guarantees to prevent re-identification

Question – which type does your research or contract require?

Questions to ask

- Do you need all of the data?
  - Can you remove some elements before applying other controls?
- Can you use
  - Synthetic data
  - Masking (substitution with similar but fictitious data)
- Or can you eliminate some data, in addition to:
  - De-identify
  - Encrypt
  - Etc.
- Cell size suppression
  - Sample sizes that are too small put identities at risk
  - Cell sizes where n is less than 10, must not be published, per UC Policy 320-40
  - https://ucdavispolicy.ellucid.com/documents/view/419/active

Toxic Data Combination

- When multiple pieces of sensitive information converge within a particular area, it creates what is known as “toxic combinations” – unnecessarily elevating your data risk profile.
- For example, having credit card numbers, names, and addresses colocated together either in a table or within the same Google Doc servers is a very toxic combination.
- It’s a critical data security concern that demands your focused attention and prioritization.

Neil Patel, Head of Global Product Marketing, BigID.com

Lessons Learned – time needed to classify

- May take several rounds of information exchange
- Often requires further clarification about data elements
- Are all data elements listed (often not)
- How is the data used?
- With what other information is it associated?
- Any contractual requirements to protect?

D'Artagnan, Athos, Aramis, and Porthos

Image by Maurice Leloir

Lessons Learned – Credit Card Information

- The P4 data classification is not enough
- PCI DSS requirements apply
  - Special contractual language
  - Special (often severe) impacts and consequences of breach or non-compliance
  - One non-compliant, all non-compliant

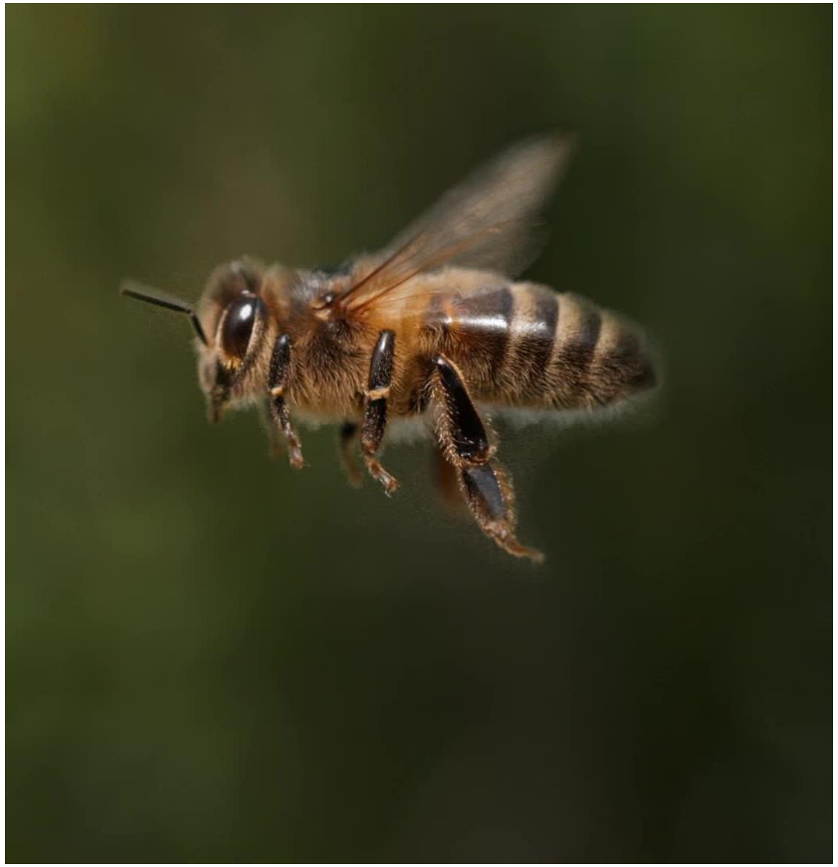
Bottom line…………..failure of one impacts all

PII

- Personally Identifiable Information
- Typically will be P3, unless directory information (P2)
- Would be P4 if associated with P4 data elements
- Public only if consent is provided, or a valid authority determined it to be so, intended for public use
- Or if unauthorized disclosure or modification could result in significant fines, penalties, regulatory action, or civil or criminal violations; statutory, regulatory and contract obligations apply; there is risk of significant harm or impairment to UC students, patients, research subjects, employees, guests/program participants, UC reputation, the overall operation of the Location or essential services, it is prudent to apply highest standard of protection.

Honeybee Data, or is it?

- Depends on use case
- Could be P1 to at least P3
- Does it fall under animal health records?
- Is it part of confidential research or public communications to alert the public about the declining bee populations?
- What protocols are in place for specific use cases?
- Animal research protocols require P3 data protection.
- Or is the data about the bee keepers?
  - Is the address a business or private home?
  - Do any of the keepers require protection for other reasons?
  - More than name, address, e-mail and phone?
  - Refer to January and February seminars for implications

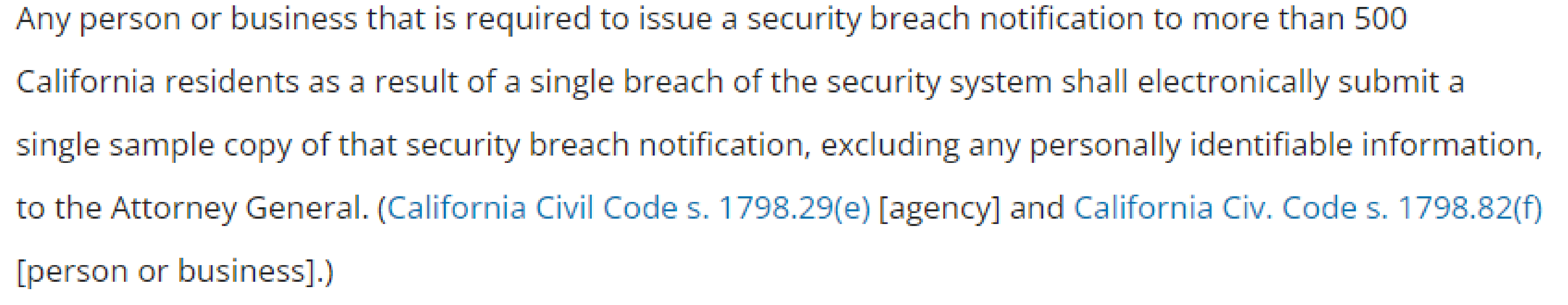


Lessons Learned – Supplier perspective

- Push back on Appendix DS Exhibits that show data types
- Treating all data the same way
- Disclaimers that services do not handle sensitive information
- Resistance to responsibility for data in UC Davis systems

Lessons Learned – Number of Records

- Can increase data classification and protection requirements
- May impact notification requirements



Any person or business that is required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. (California Civil Code s. 1798.29(e) [agency] and California Civ. Code s. 1798.82(f) [person or business].)

Lessons Learned – Privacy

- Not the same as security
- Privacy policies on supplier websites may not be what applies to contract
- Ask for privacy policy that will be associated with the contract

Monthly Seminar Topics

- Video/audio of human subjects, minors, infants, specific medical conditions, disabilities
- Remote exam proctoring
- Impact of AI on de-identifying information, facial recognition
- Mental health counseling notes
- Sports club injury information
- Honey bee health data

Seminar Meeting Schedule

January 2/28/2024 @ 2:00 PM

February 2/26/2024 @ 2:00 PM

March 2/25/2024 @ 2:00 PM

April 2/22/2024 (2nd to last Monday)

May 2/27/2024 @ 2:00 PM

June 2/24/2024 @ 2:00 PM

July 2/29/2024 @ 2:00 PM

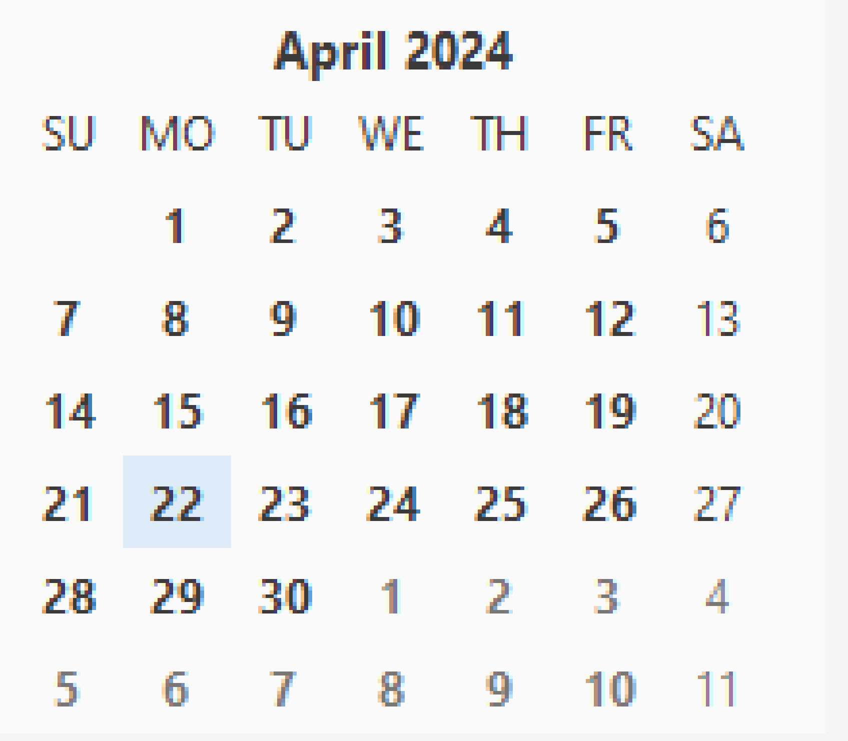
August 2/26/2024 @ 2:00 PM

September 2/30/2024 @ 2:00 PM

October 2/28/2024 @ 2:00 PM

November 2/18/2024 (2nd to last) @ 2:00 PM

December 2/16/2024 (3rd Monday) @ 2:00 PM



April 2024

SU	MO	TU	WE	TH	FR	SA
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4
5	6	7	8	9	10	11