Play an Active Role:
Tips to Incorporate Cyber Security and Privacy into Your Daily Life Today!

Robert Smith, UCOP
Systemwide IT Policy Director

Tawny Luu, UCI
Director, Public Records Office / Campus Privacy Official

Tessa Mendez, UCSB
Policy Coordinator/ Campus Privacy Official

Play an Active Role:
Tips to Incorporate Cyber Security and Privacy into Your Daily Life Today!

The views expressed are our own.

Opinions expressed are solely our own and do not express the views or opinions of the University of California.

Information stewardship is a shared responsibility.

1. Expand your toolkit
2. Grab attention
3. Make it relevant
4. Golden rule
5. Educate others
6. Do you need it?
7. Map your data
8. Records disposition
9. On/Off boarding
10. Values and Principles

1. Expand your toolkit

Do not be afraid to use all available resources

Do not be afraid to use all available resources

- There are great resources online.
  - These range from Amazon to NIST. SANS to DHS.

Do not be afraid to use all available resources

- Use humor and cartoons where they drive home the message

1. Expand your toolkit
2. Grab attention

Look for stories that grab attention

Long copy does not sell

Keep it short and pull out the most important point(s)

An edu or gov story is better than a corporate one

For example, the Target breach. Lots of things went wrong…

What is the most important point? What is the lesson that could change behavior?

Look for stories that grab attention

Staff and work place practice matters!

35%

At a September HIST/HHS HIPAA conference, the Cedars-Sinai CIO noted - 35% of patient data breaches in 2013 due to loss or theft of unencrypted laptop or other device. Hackers aren't the only threat.

43%

Assets are stolen most often from **victim work areas** according to the Verizon Data Breach Investigation Report – 43%!

20%

Miscellaneous errors by staff account to **20%** of the incidents in **education** according to the report.

2015 Verizon Data Breach Report

10 = 97%

Top 10 Common vulnerabilities accounted for 97% of all exploits

1 Year!

Most were known and had a remedy available for 1+ year!

Organization's need to rethink their patching strategy!

In June 2014, Indianapolis-based **Butler University** warned more than **160,000** students, alumni, faculty, staff, and past applicants that their personal information was exposed during a data breach in **2013**! Butler hired outside investigators, who determined that the school's network was compromised in November 2013, and remained in an exposed state until May 2014. Additional investigation into the matter showed that files containing names, dates of birth, Social Security numbers, and bank account details were also compromised. "Unfortunately, we do think it's a remote hacking. The suspect that's been arrested has no affiliation with Butler University," Michael Kaltenmark, a university spokesperson, told local NBC affiliate, WTHR.

In March of 2014, The Chronicle of Higher Education ran the headline, "*Data Breaches Put a Dent in Colleges' Finances as Well as Reputations.*" Key excerpts:

> Feb 19, 2014 - The costs of a cyber-attack on the University of Maryland that was made public last month will run into the **millions of dollars**, according to data-security professionals who work in higher education. Such a financial and reputational wallop threatens many colleges that are vulnerable to serious data breaches, experts say.
>
> The Maryland case is one of several data-security breaches reported by colleges in recent weeks. On February 25, Indiana University said a staff error had left information on **146,000** students exposed for 11 months. A week later, the North Dakota University system reported that a server containing the information of **291,465** former, current, and aspiring students and 784 employees had been hacked.
>
> Data breaches in higher education cost colleges an average of $111 per record—a figure that calculates in the damage to the institution's reputation—according to a 2013 study published by the Ponemon Institute, which studies cybersecurity.

“Your workforce is a potential vulnerability to your network.

Constantly educating your workforce and testing their cyberhygiene is very important.”

- Ari Baranoff, *Assistant Special Agent in charge of the U.S. Secret Service’s Criminal Investigative Division.*

1. Expand your toolkit
2. Grab attention
3. **Make it relevant**

“The user is going to pick dancing pigs over security every time.”

- **Bruce Schneier, *security guru and author***

Make it relevant

Connect with your users

Make them suspicious by connecting the dots

Tell them how this can happen to them.

Why?

- **Unpatched and unsupported software!**
- **This could have been my campus during a 2011 compromise.**
- **The number of records – 2,700, is something that could happen to us at any time.**
- ***Our risk assessment identified a gap in applying patches and upgrades (edited for this presentation)***
- **This is a non-profit – not a large corporation.**
- **It signals OCR's seriousness and steeper fines in these cases.**
- **$150,000**

Hello,¶
¶
I·saw·this·and·thought·it·worth·sharing.¶
¶
December·2014¶
¶
U.S.·Department·of·Health·and·Human·Services¶
¶
Office·for·Civil·Rights¶
¶
BULLETIN:°·HIPAA·Settlement·Underscores·the·Vulnerability·of·Unpatched·and·Unsupported·Software¶
¶
¶
Anchorage·Community·Mental·Health·Services·(ACMHS)·has·agreed·to·settle·potential·violations·of·the·Health·Insurance·Portability·and·Accountability·Act·of·1996·(HIPAA)·Security·Rule·with·the·Department·of·Health·and·Human·Services·(HHS),·Office·for·Civil·Rights·(OCR).°·ACMHS·will·pay·$150,000·and·adopt·a·corrective·action·plan·to·correct·deficiencies·in·its·HIPAA·compliance·program.°·ACMHS·is·a·five-facility,·nonprofit·organization·providing·behavioral·health·care·services·to·children,·adults,·and·families·in·Anchorage,·Alaska.¶
¶
¶
OCR·opened·an·investigation·after·receiving·notification·from·ACMHS·regarding·a·breach·of·unsecured·electronic·protected·health·information·(ePHI)·affecting·2,743·individuals·due·to·malware·compromising·the·security·of·its·information·technology·resources.°·OCR's·investigation·revealed·that·ACMHS·had·adopted·sample·Security·Rule·policies·and·procedures·in·2005,·but·these·were·not·followed.°·Moreover,·the·security·incident·was·the·direct·result·of·ACMHS·failing·to·identify·and·address·basic·risks,·such·as·not·regularly·updating·their·IT·resources·with·available·patches·and·running·outdated,·unsupported·software.¶
¶
"Successful·HIPAA·compliance·requires·a·common·sense·approach·to·assessing·and·addressing·the·risks·to·ePHI·on·a·regular·basis,"·said·OCR·Director·Jocelyn·Samuels.°·"This·includes·reviewing·systems·for·unpatched·vulnerabilities·and·unsupported·software·that·can·leave·patient·information·susceptible·to·malware·and·other·risks."¶
¶
ACMHS·cooperated·with·OCR·throughout·its·investigation·and·has·been·responsive·to·technical·assistance·provided·to·date.°·In·addition·to·the·$150,000·settlement·amount,·the·agreement·includes·a·corrective·action·plan·and·requires·ACMHS·to·report·on·the·state·of·its·compliance·to·OCR·for·a·two-year·period.°·The·Resolution·Agreement·can·be·found·on·the·OCR·website·at·http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html¶
¶
This·is·noteworthy·because:¶

1. This·could·have·been·us·during·the·2011·compromise.¶
2. The·number·of·records—2,700,·is·something·that·could·happened·to·us·at·any·time.¶
3. *Our·risk·assessment·identified·a·gap·in·applying·patches·and·upgrades·(edited·for·this·presentation)*¶
4. This·is·a·non-profit—·not·a·large·corporation.¶
5. It·signals·OCR's·seriousness·and·steeper·fines·in·these·cases.¶

Costs related to data-security lapses dating to 2011 at the **Maricopa County Community College District**, in Arizona, could climb to **$17.1-million**, says Tom Gariepy, a district spokesman. Trustees have approved contracts including **$2.25-million** for Oracle to repair the network, up to **$2.7-million** in legal expenses, and up to **$7-million** for notification and credit-monitoring services, among other costs. The district has received notice of a class-action lawsuit. 2.4 million records were stolen!

Later the costs were reported at $26 million!

Alaska settles HIPAA security case for $1,700,000

The Alaska Department of Health and Social Services (DHSS) has agreed to pay the U.S. Department of Health and Human Services' (HHS) $1,700,000 to settle **possible** violations of the HIPAA Security Rule.

The HHS Office for Civil Rights (OCR) began its investigation following a breach report submitted by Alaska DHSS

The report indicated that a portable electronic storage device (USB hard drive) **possibly** containing ePHI was stolen from the vehicle of a DHSS employee.

OCR found evidence that DHSS did not have adequate policies and procedures in place to safeguard ePHI.

The evidence indicated that DHSS had not completed a risk analysis, implemented sufficient risk management measures, completed security training for its workforce members, implemented device and media controls, or addressed device and media encryption as required by the HIPAA Security Rule.

The issues:
If a USB drive is lost it does not matter if there is ePHI on it – it matters if you know! And have a policy that says you know! Your risk analysis must address at this granularity – does it?

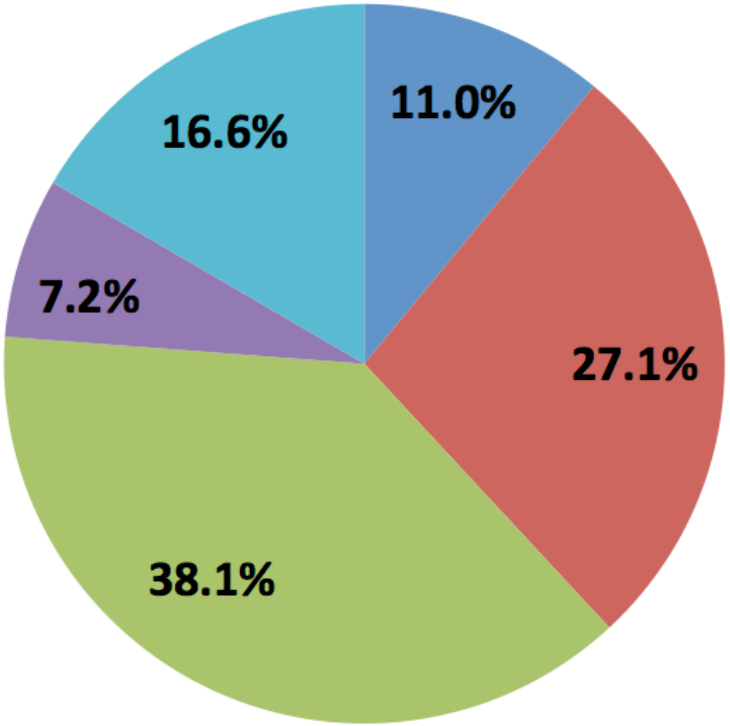
1. Expand your toolkit
2. Grab attention
3. Make it relevant
4. **Golden rule**

Treat the data you are handling as if it were data about yourself

1. Expand your toolkit
2. Grab attention
3. Make it relevant
4. Golden rule
5. **Educate others**

Start your own campaign to educate others that data protection is not just an IT issue

What was the source of the last data breach your organization suffered?



- A hacktivist or hacker
- Lost device – memory stick, laptop, DVD, etc.
- Lost paper files
- A data processor your organization uses was breached
- A vendor or supplier (other than a data processor) had the breach

www.corporatecompliance.org

10 Risky Practices Employees Routinely Engage In

1. Connecting computers to the Internet through an insecure wireless network.
2.Not deleting information on their computer when no longer necessary.
3.Sharing passwords with others.
4.Reusing the same password and username on different websites.
5.Using generic USB drives not encrypted or safeguarded by other means.
6.Leaving computers unattended when outside the workplace.
7.Losing a USB drive possibly containing confidential data and not immediately notifying their organization.
8.Working on a laptop when traveling and not using a privacy screen.
9.Carrying unnecessary sensitive information on a laptop when traveling.
10.Using personally owned mobile devices that connect to their organization's network.

Ponemon Institute Study titled "The Human Factor in Data Protection"

1. Expand your toolkit
2. Grab attention
3. Make it relevant
4. Golden rule
5. Educate others
6. **Do you need it?**

When collecting personal information ask yourself if you really need it to do your job

1. Expand your toolkit
2. Grab attention
3. Make it relevant
4. Golden rule
5. Educate others
6. Do you need it?
7. **Map your data**

Know where your data are

The best way to protect confidential information…

1. Expand your toolkit
2. Grab attention
3. Make it relevant
4. Golden rule
5. Educate others
6. Do you need it?
7. Map your data
8. **Records disposition**

…is not to have it at all.

IDENTIFY

the records you have

- Distinguish between records and non-records
- Identify the people who use the documents to determine whether they are still in use
- Label your files accurately
- Use a common naming standard
  YYYY-MM-DD

CHECK

the UC Record Retention Schedule

The Retention Schedule can be found at: http://recordsretention.ucop.edu/

If you are unsure how to use the retention schedule, you can watch a taped webinar: http://www.ucop.edu/information-technology-services/initiatives/records-retention-management/training-materials.html

UNIVERSITY OF CALIFORNIA

Records Retention Schedule

SEARCH THE SCHEDULE

Search

BROWSE THE SCHEDULE

Browse by Category

ACCESS THE FULL SCHEDULE

Full Schedule
Print Full Schedule

RESOURCES

Retention Schedule FAQs (PDF)
Retention Schedule Glossary (PDF)
Contact
Home

ANNOUNCEMENTS

3/21/2014 (PDF)
8/1/2013 (PDF)

About the Schedule

Knowing what records to keep and for how long is challenging. A records retention sche
destroyed. Various requirements based in law and university policy govern the retention
management, mitigating risk, and ensuring consistent compliance across UC. The Unive
the universitywide records retention schedule. To gain an understanding on how to use
the appropriate campus Records Management Coordinator .

It is important for all members of the University community to adhere to the retention per
lawful authorization for the disposition of records; consequences of not following the sch

Schedule update project
The RMC currently is conducting a systemwide project to update the records retention s

Records included in the schedule
Per University policy, RMP-1, "University Records Management Program," and except a
schedule applies to all administrative records, regardless of their medium, owned by the

- University of California campuses and the Office of the President,
- University of California health sciences centers, and
- Department of Energy laboratories managed by the University of California.

The schedule does not apply to

- Administrative records held by the Principal Officers of The Regents,
- Teaching and research records (e.g., library materials, faculty research and teach
- Records pertaining to individual patient care (medical records).

Records holds
If pending, foreseeable, or ongoing litigation; an investigation; or an ongoing audit pertai

UNIVERSITY OF CALIFORNIA

SEARCH THE SCHED

BROWSE THE SCHED
Browse by Category

ACCESS THE FULL S
Full Schedule
Print Full Schedule

RESOURCES
Retention Schedule FA
Retention Schedule Gl
Contact
Home

ANNOUNCEMENTS
3/21/2014 (PDF)
8/1/2013 (PDF)

seded are in this database.

Function:
04. Human Resources Records

Function Description:
Human Resources Records document the human resources processes and activities of the University, such as recruitment, employment, and separation activities of employees from the University. They also document human resources transactions managed through the University.

Category:
B. Individual Employee Employment and Interns, Volunteers and Contingent Workers Records

Category Description:
Individual Employee Employment and Interns, Volunteers and Contingent Workers Records document each individual employee's, intern's, volunteer's or contingent worker's work history with the University. This would include full time employees, part time employees, temporary employees, student employees including Federal Work Study funded positions, interns and volunteers. These records found in all media (paper, electronic, or otherwise) may include but are not limited to:
• hiring negotiation and employment contract records;
• background check records and other on-boarding records, including the Employment Eligibility Verification Form (I-9), Patent Agreement and Oath;
• performance related records including records for training and other professional/staff development that is mandatorily required to maintain employment, special recognition and merit records, counseling memos and evaluations (disciplinary records are found in C. Employment Related Claims Records); and
• records documenting changes in employment due to various circumstances such as reasonable accommodations, telecommuting, flexible schedules, promotions, demotions, transfers, reclassifications, resignations, discharges and retirements.

Sub-Category Title:
B. 1. Mandatory training and other professional/staff development records

Keywords:
training, professional development, staff development, Employee Training, Faculty Training, Mandatory Training, Police Training, Professional Development, Safety Employee Training, Staff Development Program, Staff Training, Training Conference, Training Seminar

Retention Period:
Official Record: Retain records for 5 years after the end of the fiscal year in which the training takes place. All Other Copies: Copies are considered non- records, and should be retained only until their usefulness has passed, but never any longer than the official record.

Retention Rule:
Delete or destroy after the retention period has lapsed

Primary Owner:

Public Retention Schedule - Approved Date:
2014-09-19

Category Description	Sub-Category Title	Keywords	Retention Period
Pre-employment and Recruitment Records document the activities surrounding the selection processes more...		Pre-employment, Recruitment Records, search records, selection records, announcements records, more...	Official Retain years end of year in specifi
Individual Employee Employment and Interns, Volunteers and Contingent Workers Records document mor...	B. 1. Mandatory training and other professional/staff development records	training, professional development, staff development, Employee Training, Faculty Training, more...	Official Retain for 5 y the en fiscal y which training
Individual Employee Employment and Interns, Volunteers and Contingent Workers Records document mor...	B. 2. Background Check Records	Candidate Background Check, background check records, on- boarding records, Background check, more...	Official Retain for 5 y the en fiscal y which
Individual Employee	B. 3. Intern, Volunteer and	Interns, Volunteers,	Official Retain

DETERMINE

whether the records can be destroyed

The retention period has lapsed, and no one uses the records…	**Destroy or delete the records. Shred sensitive, confidential, or restricted paper records.**
The retention period has lapsed, but people still use the records…	**Contact your local records manager**
The retention period has lapsed, but they are part of an ongoing litigation, investigation, PRA request, or audit…	**Keep the records.**

Remember- you should NOT destroy a record if there is:

- A public records act request;
- Pending, foreseeable, or ongoing litigation;
- An investigation; or
- An ongoing audit pertaining to the records is taking place.

This is called a “records freeze.” The records cannot be destroyed under the Record Retention Schedule until these actions have been completed or resolved.

1. Expand your toolkit
2. Grab attention
3. Make it relevant
4. Golden rule
5. Educate others
6. Do you need it?
7. Map your data
8. Records disposition
9. **On/Off boarding**

Focus on privacy and security at the beginning and end of the employment relationship

Onboarding

- Define security responsibilities in job descriptions
- Carry out screening and background checks in accordance with law and policy
- Use confidentiality and security agreements stating responsibilities for security and privacy
- Document access rights granted
- Set expectations for certifications, continuing education, memberships, and subscriptions
- Provide education, awareness, and training

ISO 27002 (formerly 17799)

“The financial value of employee awareness is even more compelling. Organizations that do not have security awareness programs—in particular, training for new employees—report significantly higher average financial losses from cybersecurity incidents. Companies without security training for new hires reported average annual financial losses of $683,000, while those do have training said their average financial losses totaled $162,000.”

PwC, “US Cybercrime: Rising Risks, Reduced Readiness”
http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf

$500,000

The Bottom Line

Offboarding

- Collect keys, ID cards, mobile devices, credit cards, software, and information stored on electronic media
- Change passwords on generic accounts
- Adjust or remove access rights of the separated employee
- Document the removal of access to systems

ISO 27002 (formerly 17799)

Reference UC Values and Principles

1. Expand your toolkit
2. Grab attention
3. Make it relevant
4. Golden rule
5. Educate others
6. Do you need it?
7. Map your data
8. Records disposition
9. On/Off boarding
10. Values & Principles

Ethics, Compliance and Audit Services

COMPLIANCE

Overview & key elements

Clery Act (Campus safety and crime reporting)

Health sciences compliance

Health Insurance Portability and Accountability Act (HIPAA)

International compliance

Privacy ›

Research compliance

Privacy principles & practices at UC

The University of California makes every effort to respect the privacy of individuals. Pri integral to human dignity and necessary for an ethical and respectful workplace. The ri privacy is also declared in the California Constitution. To this end, the University works integrate best practices across its organization at the systemwide and campus levels. T section defines privacy principles and practices at UC and contains resources from the of the President, UC campuses, and governmental agencies on the main areas of privac UC.

Privacy at UC Campuses: All UC campuses have designated a Campus Privacy Official. Privacy Official is the local campus administrative resource for implementing privacy b practices at that campus.

What does privacy mean at UC? Privacy consists of (1) the individual's ability to condu activities without concern of or actual observation and (2) the appropriate protection, and release of information about individuals. (Read more about UC Privacy Principles)

For more information: View the links below for additional details, and/or contact your campus privacy official.

1. UC Statement of Privacy Values

Overview

The UC Statement of Privacy Values first declares privacy as an important value of the University of California. It then defines what the two forms of privacy are, and explains that they must be balanced with one another and with other values and obligations of the University. To give context, the values of academic and intellectual freedom are highlighted as fundamental to an educational and research institution; and the values of transparency and accountability are highlighted as fundamental to a public institution. Finally, a summary of elements that the University strives to balance appropriately is given.

The UC Statement of Privacy Values

The University of California respects the privacy of individuals. Privacy plays an important role in human dignity and is necessary for an ethical and respectful workplace. The right to privacy is declared in the California Constitution.

Privacy consists of (1) an individual's ability to conduct activities without concern of or actual observation and (2) the appropriate protection, use, and release of information about individuals.

The University must balance its respect for both types of privacy with its other values and with legal, policy, and administrative obligations.

Academic and intellectual freedoms are values of the academy that help further the mission of the University. These freedoms are most vibrant where individuals have autonomy: where inquiry is free because it is given adequate space for experimentation and the ability to speak and participate in discourse within the academy is possible without intimidation.

Transparency and accountability are values that form the cornerstone of public trust. Access to information concerning the conduct of business in a public university and an individual's access to information concerning him/herself is a right of every citizen as stated in the California Constitution.

Thus, the University continually strives for an appropriate balance between:

- ensuring an appropriate level of privacy through its policies and practices, even as interpretations of privacy change over time;
- nurturing an environment of openness and creativity for teaching and research;
- being an attractive place to work;
- honoring its obligation as a public institution to remain transparent, accountable, and operationally effective and efficient; and
- safeguarding information about individuals and assets for which it is a steward.

Information Protection

Free Inquiry

Transparency & Notice

Surveillance

Accountability

Respect for Individual Privacy

Privacy by Design

Choice

Information Review and Correction

Questions?

1. Expand your toolkit
2. Grab attention
3. Make it relevant
4. Golden rule
5. Educate others
6. Do you need it?
7. Map your data
8. Records disposition
9. On/Off boarding
10. Values and Principles