UC DAVIS HEALTH | Compliance and Privacy Services

Privacy and Security

Annual Training

Learning Objectives

Learning Objectives

In this training, you will learn:

- What qualifies as patient information.
- Your responsibility to protect patient information.
- Situations on access, use, or disclosure (“share”) of patient information.
- The potential consequences of inappropriately accessing, using, or sharing patient information.
- The ways UC Davis Health protects patient information.
- Why it’s important to protect patient information.

What Qualifies as Patient Information?

1 2 3

Select each button to explore some common* types of patient information.

* Patient information is not limited to these examples.

What Qualifies as Patient Information?

1 2 3

Select each button to explore some common* types of patient information.

* Patient information is not limited to these examples.

What Qualifies as Patient Information?

Direct Interaction with a Patient
Including talking to or examining a patient at a visit.

What Qualifies as Patient Information?

Discussions About Patients
Including conversations about a patient's health or treatment with the patient, their family, or another health care provider.

What Qualifies as Patient Information?

Medical Records
Documents, images, and other items that keep track of a patient's healthcare.

Laws and Policy

Laws and Policy

UC Davis Health must protect **patient information** by law and policy.

Federal

State

Policy

Select each image above to review the rules guiding how, why, and when we protect patient information.

Laws and Policy

UC Davis Health must protect **patient information** by law and policy.

Federal

State

Policy

Select each image above to review the rules guiding how, why, and when we protect patient information.

Federal Laws

- Health Insurance Portability and Accountability Act **(HIPAA)** and its regulations
  - Privacy Rule
  - Security Rule
  - Breach Notification Rule
- Health Information Technology for Economic and Clinical Health Act **(HITECH)**
- HIPAA Omnibus Rule

State Laws

- Confidentiality of Medical Information Act **(CMIA)**
- Information Practices Act **(IPA)**

Laws and Policy

UC Davis Health must protect **patient information** by law and policy.

UC, UC Davis, and UC Davis Health policies guide how, why, and when we protect patient information.

Policy

Key Terms

Key Terms

Click on each key terms to learn the difference between various types of information we handle and work to protect.

UC DAVIS HEALTH

Individually identifiable

Information is **individually identifiable** if alone or combined with public information it can reveal a person's identity.

Even without a name or birthdate, information can still identify someone if people can sufficiently guess who is involved by using the news, internet searches, or social media content.

Need more details?

For full definitions of these terms, please see UC Davis Health policy 2902, Confidentiality.

Protected Health Information (PHI)

PHI is the term used in **HIPAA**. PHI is any information that identifies a person or could be used to identify them, **coupled with:**

- Their past, present, or future physical or mental health condition(s)
- Their health care, or
- Payment for their health care

Need more details?

For full definitions of these terms, please see UC Davis Health policy 2902, Confidentiality.

Medical Information

California medical law uses the term "medical information" instead of PHI.

Medical information is any individually identifying information about a patient's health, medical history, or treatment.

Need more details?

For full definitions of these terms, please see UC Davis Health policy 2902, Confidentiality.

Personal Information (PI)

PI is another key term used in California privacy law and **applies to all persons, including the workforce.**

PI is any information that identifies or describes a person, and statements made by, or associated with, the individual, such as:

name, social security number, physical description, home address, telephone number, education, financial matters, medical or employment history.

Remember: PI is confidential, even if it doesn't include any medical or health information.

Notice of Privacy Practices

Notice of Privacy Practices

Distributing the NPP

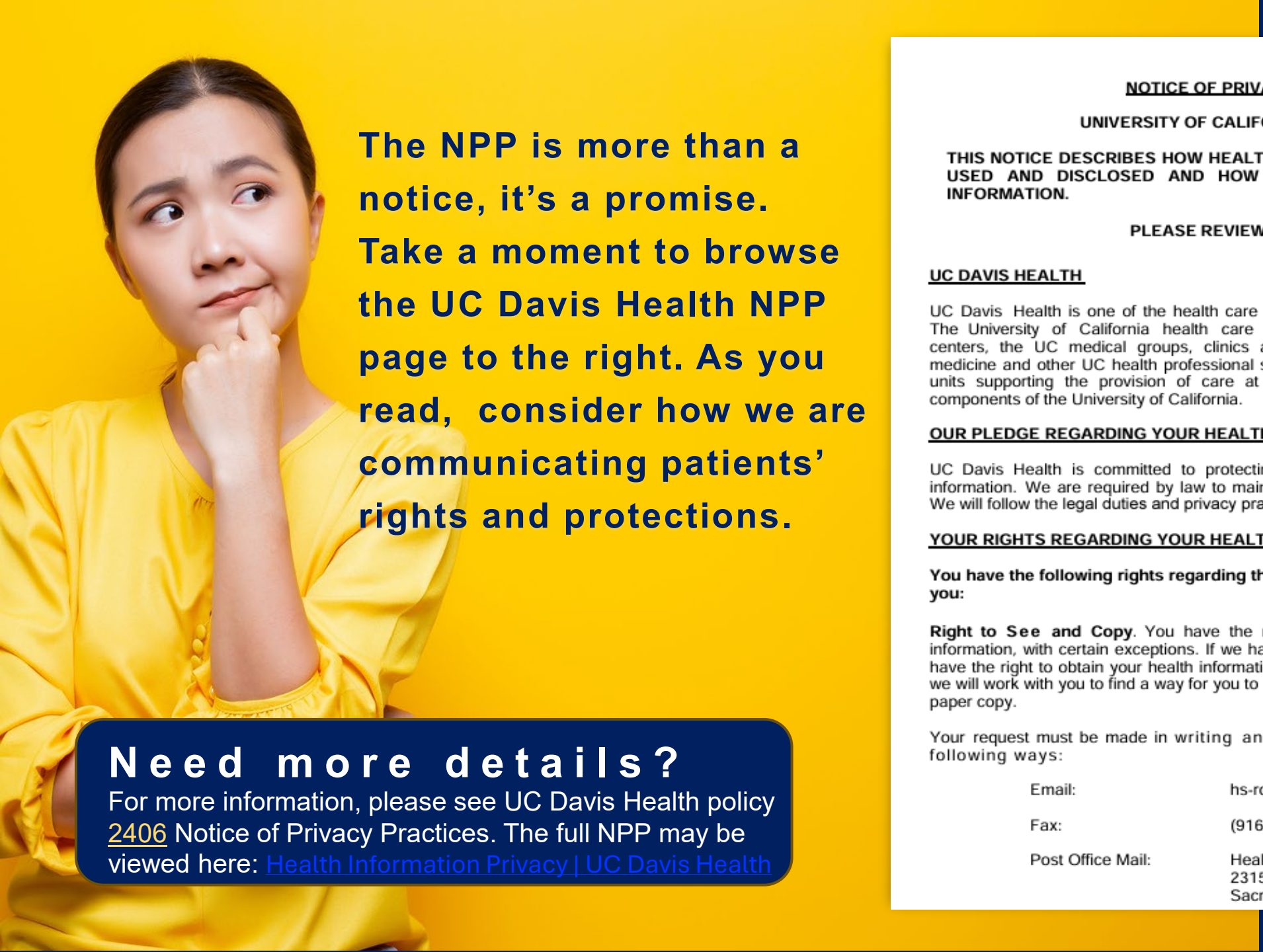
As a Covered Entity, to use and share patient information UC Davis Health should first give each patient a Notice of Privacy Practices (NPP).

Contents of the NPP

The NPP explains how the information may be used or shared and the rights the patient has related to their information.

Documenting Patient Acknowledgement

The patient should be asked at their first visit to sign for receipt of the NPP, unless it's an emergency and the signature can't be obtained. If the signature isn't obtained while the patient is visiting, the reason must be documented in the patient's electronic medical record (EMR) and the document should be promptly mailed or electronically sent to the patient.



The NPP is more than a notice, it's a promise. Take a moment to browse the UC Davis Health NPP page to the right. As you read, consider how we are communicating patients' rights and protections.

Need more details?

For more information, please see UC Davis Health policy 2406 Notice of Privacy Practices. The full NPP may be viewed here: Health Information Privacy | UC Davis Health

NOTICE OF PRIVACY PRACTICES

UNIVERSITY OF CALIFORNIA DAVIS HEALTH

THIS NOTICE DESCRIBES HOW HEALTH INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.

PLEASE REVIEW IT CAREFULLY

UC DAVIS HEALTH

UC Davis Health is one of the health care components of the University of California. The University of California health care components consist of the UC medical centers, the UC medical groups, clinics and physician offices, the UC schools of medicine and other UC health professional schools. The administrative and operational units supporting the provision of care at all locations listed are also health care components of the University of California.

OUR PLEDGE REGARDING YOUR HEALTH INFORMATION

UC Davis Health is committed to protecting the privacy of your medical and health information. We are required by law to maintain the privacy of your health information. We will follow the legal duties and privacy practices described in this notice ("Notice").

YOUR RIGHTS REGARDING YOUR HEALTH INFORMATION

You have the following rights regarding the Health Information we maintain about you:

Right to See and Copy. You have the right to see or get a copy of your health information, with certain exceptions. If we have the information in electronic format, you have the right to obtain your health information in an electronic format if possible. If not, we will work with you to find a way for you to receive the information electronically or as a paper copy.

Your request must be made in writing and submitted through any one of the following ways:

Email:	hs-roi@ucdavis.edu
Fax:	(916) 734-2126
Post Office Mail:	Health Information Management 2315 Stockton Blvd. Sacramento, CA 95817

Patient Rights

HIPAA and state law list certain patient rights about the access, use, and sharing of patient information, to include a right to:

- Inspect and copy information in their Designated Record Set (DRS)
- Request a copy of their medical record
- Request an addendum or amendment to their medical record
- Request an Accounting of Disclosures of their information
- Request restrictions to specific uses and disclosures of their information
- Request confidential communications of their information
- Request a paper copy of the Notice of Privacy Practices (NPP)
- Submit a complaint about potential violations of their privacy
- Be notified of a Breach

For more information, please review UC Davis Health policy 2379, Patient Rights Related to Protected Health Information. Also visit the Health Information Management (HIM) webpage.

UC DAVIS HEALTH

When and how can I access, use, and/or share Patient Information?

click here

Patient Authorization

click here

Treatment, Payment, and Operations (TPO)

Select each button above to learn more about Patient Authorization and TPO.

When and how can I access, use, and/or share Patient Information?

click here

Patient Authorization

click here

Treatment, Payment, and Operations (TPO)

Select each button above to learn more about Patient Authorization and TPO.

Patient Authorization

Patient Authorization

An important part of privacy laws that gives patients control over their information is the patient authorization. There are several types of patient authorization for specific scenarios, as listed in the next slide.

Generally, we must get written permission from a patient or their legal representative before we can access, use, or share their PHI *unless* doing so is for treatment, payment, or healthcare operations (TPO).

Patient Authorization

For example, unless we have prior written permission or TPO applies, we generally may **not** share a patient's information with :

- a family member/friend
- an employer
- a lawyer/agent
- a researcher for use in a research study
- a company for use in our marketing or advertising campaigns

Did you know?

HIPAA and state law have specific requirements for a written authorization.

For more information, please review the following:

Health Information Management (HIM)
UC Davis Health policy 2414, Disclosing Protected Health Information by a Valid HIPAA Authorization;

Public Affairs and Marketing
UC Davis Health policy 1426, Photography, Recordings, and Protected Health Information – Obtaining Consent and Authorization

UC Davis Office of Research – Research Authorization form
For more information and other forms: Forms

Treatment, Payment, and Operations (TPO)

Treatment, Payment, and Operations (TPO)

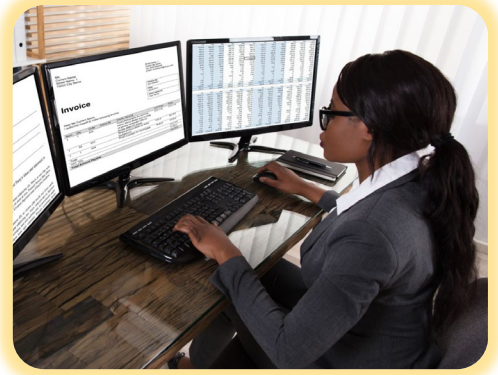
Treatment means providing, coordinating, or managing a patient's health care. This includes, but is not limited to:

- Giving the patient direct care
- Providers talking to each other about the patient's care for work purposes
- Referring the patient to another provider for continuation of care

Treatment, Payment, and Operations (TPO)

Examples of payment activities include:

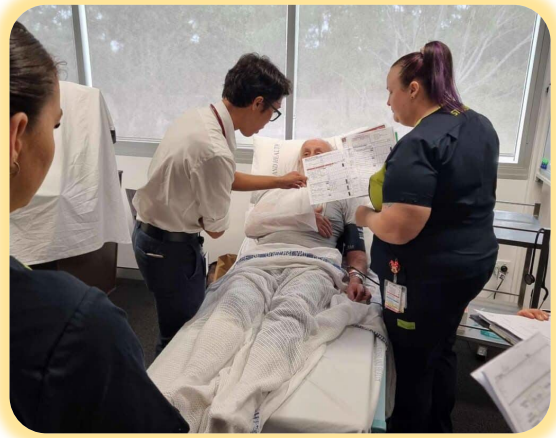
- Coding charges
- Checking if a patient is eligible for a payment and/or health plan and processing claims
- Reviewing health care services ordered for a patient to make sure they are needed, covered, and used properly
- Billing and collecting payments
- Getting payment or reimbursement for services



Treatment, Payment, and Operations (TPO)

Operations involve activities that help run the medical center, including but not limited to:

- Teaching medical students and other trainees
- Managing workforce performance and giving ongoing training
- Reviewing the work of medical staff
- Conducting internal audits
- Working on quality improvement (QI) and quality assurance (QA) projects that are not considered research



PRIVACY SPOTLIGHT

What if a patient gives me permission to *access* their patient information?

While a patient may permit you/say you can access their EMR, policy does not allow workforce members to access patient information *unless* it is for a **work-related task**.

While a patient says you can look in their EMR that doesn't mean you should if doing so is not part of **your assigned work tasks**. At minimum, this could result in a policy violation.

Key Points:

1. Access, use, and sharing of patient information is only permitted for work-related tasks.

2. Access to patient information must be limited to the minimum amount of information needed to do the work-related task at hand.

?

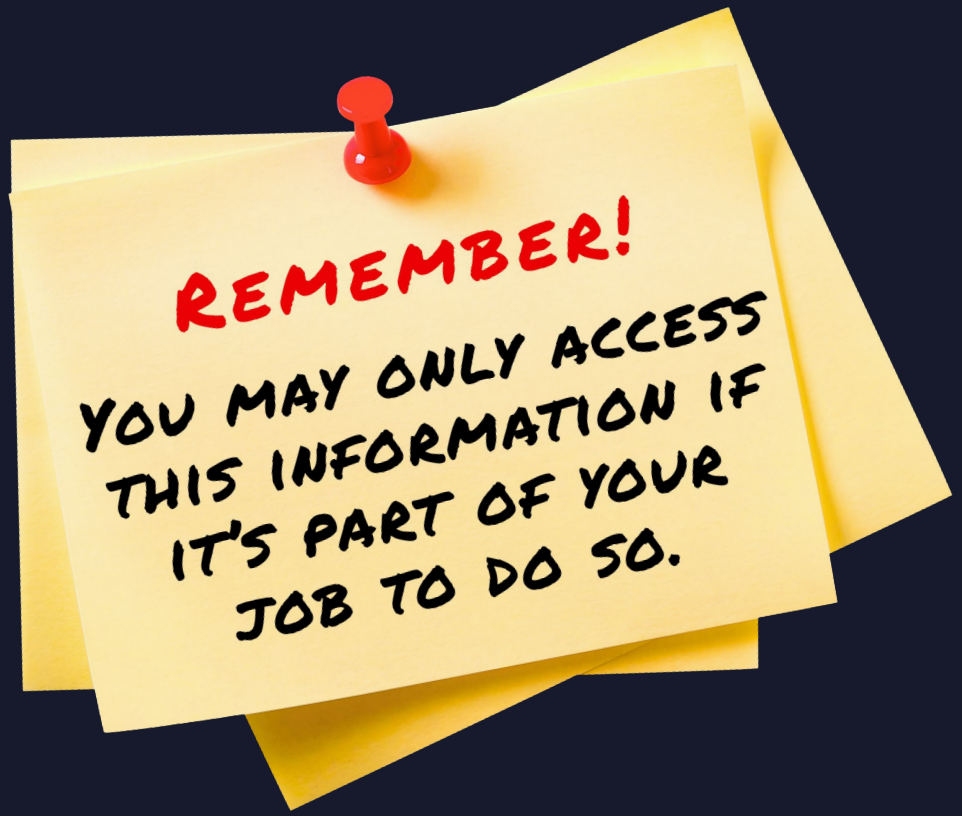
Need more details?

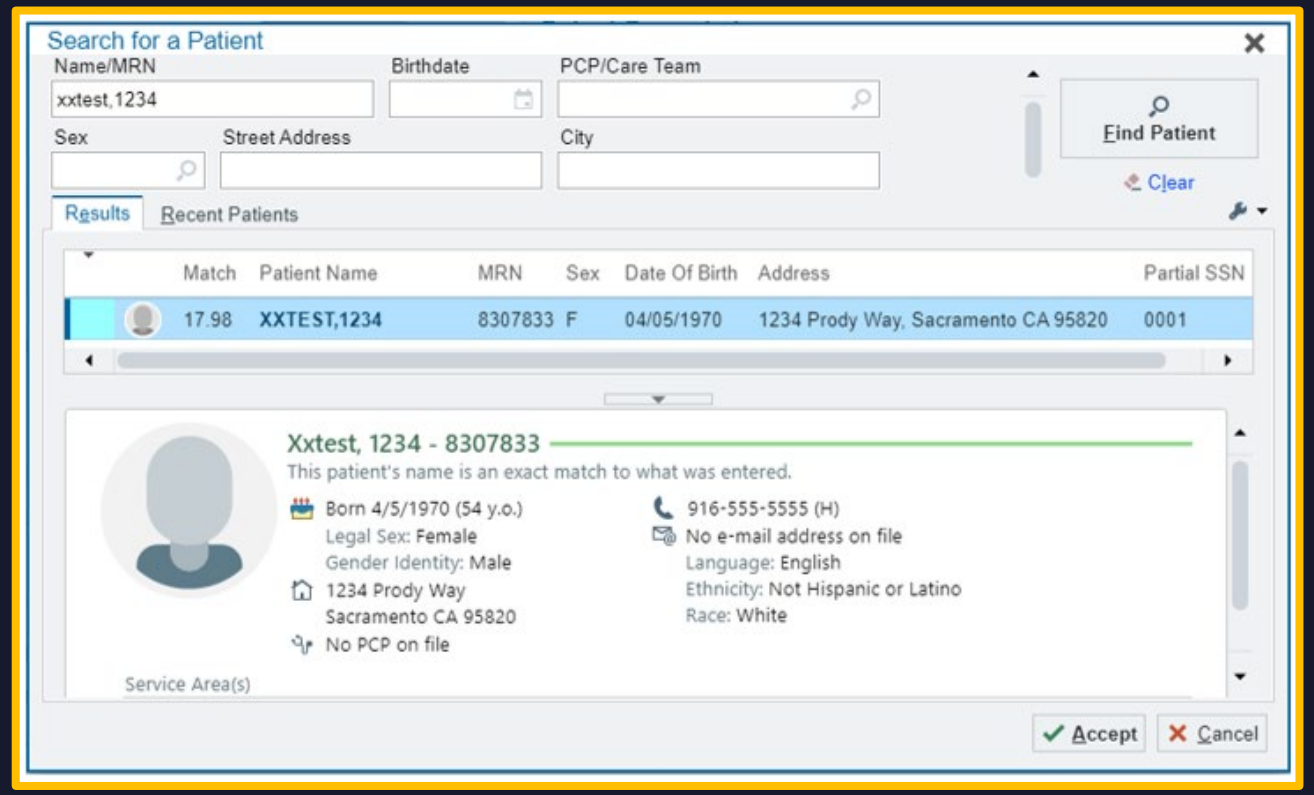
For more information, please review UC Davis Health policy 2454, Employee Access to Protected Health Information and Personal Information.

PRIVACY SPOTLIGHT

Accessing Patient Information in Epic

- All patient information in Epic, the electronic medical record (EMR) system used at UC Davis Health, is protected.
- When you search for a patient record (see below), the information returned is patient information.



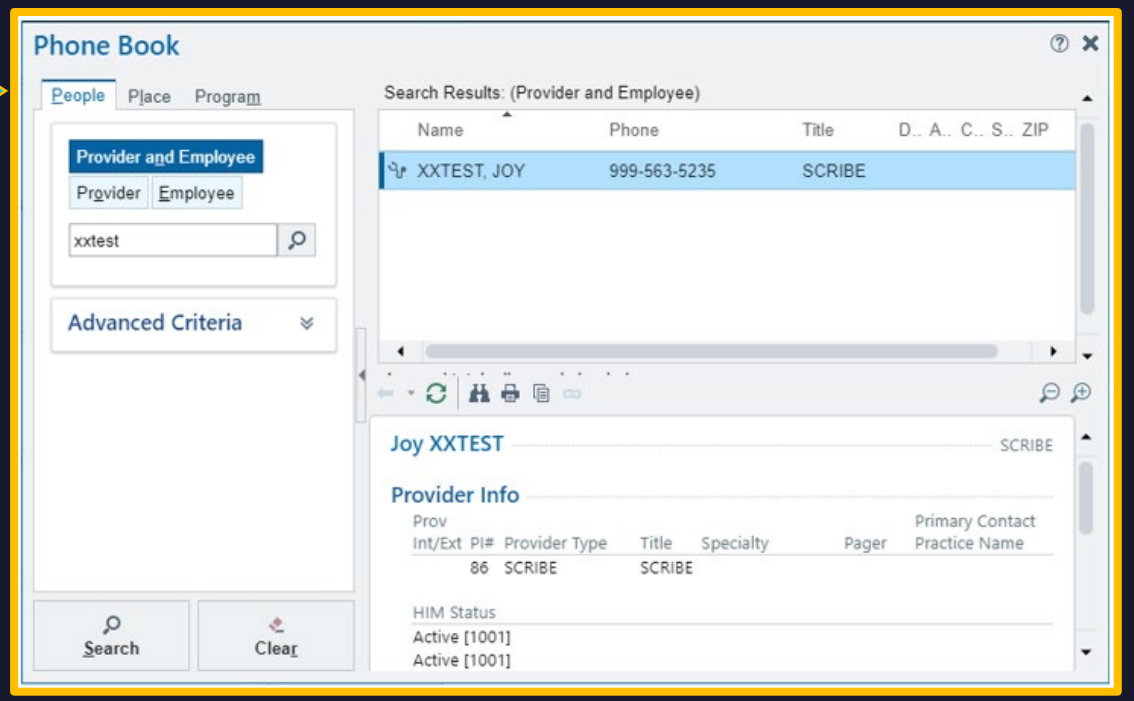


PRIVACY SPOTLIGHT

Accessing Patient Information in Epic

Never use the EMR system as a personnel directory. If you need the work contact information of a workforce member, use one of the following tools instead:

- The **Epic Phone Book**
- The Microsoft Outlook address book
- Other official UC Davis or UC Davis Health directories or contact lists



Before we move on to explore *other permitted uses and disclosures*, let's recap two key points that we've covered.

Privacy laws allow the UC Davis Health (UCDH) workforce to use and share patient information:

1. With prior patient or legal representative authorization
2. For treatment, payment, and operations (TPO)

When and *how else* can I access, use, and/or share Patient Information?

click here

Other Permitted Uses and Disclosures

click here

Special Topics

Select each button above to learn about more permissible ways you can access, use, and/or share patient information.

Other Permitted Uses and Disclosure

Click each image below to learn more about other permitted uses and disclosures.

For many of these reasons, an entry into the Disclosure Tracking database is required. For more details, please see UC Davis Health policy 2446, Tracking Disclosures of Protected Health Information.

Other Permitted Uses and Disclosure

Click each image below to learn more about other permitted uses and disclosures.

For many of these reasons, an entry into the Disclosure Tracking database is required. For more details, please see UC Davis Health policy 2446, Tracking Disclosures of Protected Health Information.

Research

Before accessing, using, or sharing patient information for a research reason, you must:

- Get IRB Approval, and
- Get Written Authorization, through either:
  - A Waiver of Authorization from the IRB; and/or
  - A signed HIPAA Authorization Form from the patient/research subject or their legal representative, plus an Informed Consent Form (ICF) as directed by the IRB.

If you cannot get IRB approval, you must get written permission from UC Davis Health Compliance and Privacy Services.

Did You Know?

When patient information is accessed or obtained under the permission of a Waiver, an **Accounting of Disclosure** entry is required.

For more details, please see UC Davis Health **policy 2446**, Tracking Disclosures of Protected Health Information.

The **UC Davis IRB** and **UC Davis Health Research Compliance** websites also provide more detailed information on this topic.

Research Health Information

- Research Health Information (RHI) is information **collected, created, and used only for a research purpose**.
- RHI exists when it is in the possession of a research team. It may come from the subject's EMR or be obtained directly from the research subject during an interaction for a research study purpose.
- This includes data from organized studies, like clinical trials or observational research. This information is not considered part of a patient's regular EMR/Designated Record Set (DRS).

Public Health Activities

The HIPAA Privacy Rule allows UC Davis Health to share patient information with public health authorities like the FDA, CDC, and OSHA without first getting patient authorization.

Examples of public health sharing include reportable diseases, injury, birth, death, public health investigations, child abuse, product safety, and workplace health/surveillance checks.

Business Associates

A Business Associate (BA) is an outside person or entity that helps UC Davis Health (UCDH) complete work activities. UCDH may share patient information with a BA after the BA signs a contract, a HIPAA-compliant Business Associate Agreement (BAA), and Data Security Agreement (DSA). The BAA and DSA require the BA to keep the information shared private and secure.

Some examples of BAs include:

- Photocopy agencies that help UCDH copy and share medical records
- Technology companies that help UCDH with network and/or computer systems
- Consultants that help UCDH with clinical operations

For more information, please review UCDH policy 2401, HIPAA Business Associate Agreement (BAA)

Law Enforcement

Your duty as a UC Davis Health (UCDH) workforce member is to the patient, not law enforcement!

Generally, a patient retains their privacy and authorization rights. However, patient information may be shared with law enforcement **without first getting a patient's authorization** to report: suspected abuse, neglect, or domestic violence; death from criminal conduct; or criminal conduct that occurs at the medical center.

For more information, please review UCDH **policy 2426**, Disclosing Protected Health Information to Law Enforcement.

Facility Directory Information

UC Davis Health is allowed to share information stored in the facility (“hospital”) directory to respond to in-person requests or calls about a patient's presence and location in the hospital.

To do so, the patient must first be informed during their hospital visit about the information that may be shared upon request and with whom. The patient can ask to limit what is shared, choose who gets it, or opt-out of the directory entirely.

In an emergency or if a patient cannot express their preference because of condition, directory information may still be shared upon request if doing so is in the patient's best interest and does not go against any known patient preference.

For more information, please review UCDH **policy 2418**, Disclosing Protected Health Information to the Media and Public.

Special Topics

The following are special topics that you should know and may need to know depending on your work role at UCDH.

Limited Data Sets

Photography and Video-recording

De-identification

Social Media

Artificial Intelligence

Confidential Patients

Click each picture above to receive a general overview of each special topic.

Questions? Please contact Compliance and Privacy Services for support.

Special Topics

The following are special topics that you should know and may need to know depending on your work role at UCDH.

Limited Data Sets

Photography and Video-recording

De-identification

Social Media

Artificial Intelligence

Confidential Patients

Click each picture above to receive a general overview of each special topic.

Questions? Please contact Compliance and Privacy Services for support.

Limited Data Sets

A Limited Data Set (LDS) is Protected Health Information (PHI) under HIPAA. Unlike de-identified information, an LDS can include dates (e.g., DOB, DOS, etc.), location of service, geographic locations (i.e., city, state, zip code), and unique identifiers that do not allow for the re-identification of a patient.

To access or use an LDS, a Data Use Agreement (DUA) must be completed. The DUA is like any contract that explains who can receive and use the LDS, how they can share it, and the rules they must follow.

The **UC Davis Office of Research** can help you complete a DUA.

Additional resources on LDS and DUA are available in the **UC Davis Clinical Research Guidebook**.

De-identification

De-identification is the process of **removing all patient identifiers** from patient information. This way, the data can be used and shared for many operational purposes without identifying the patient, and privacy risk is significantly reduced.

The HIPAA Privacy Rule includes **two (2) approved de-identification methods**:

1. Expert Determination, or
2. Safe Harbor, which means removing all **18 HIPAA recognized identifiers** and ensuring the remaining data can't be used to identify the patient.

De-identification

Fully de-identified information can also be used for a research purpose **without getting prior permission from the patient/subject**.

NOTE: IRB approval is not required to get de-identified information. but approval from UC Davis Health Compliance and Priavcy Services may still be required.

The first step to get this type of information is to submit a **ServiceNow request**.

PRIVACY SPOTLIGHT

Artificial Intelligence (AI) Tools

Artificial intelligence (AI) that creates text, video, images, audio, communications, and other content is transforming healthcare. While AI tools help improve healthcare and business processes, they also pose risks if misused by the UC Davis Health (UCDH) workforce or exploited by attackers.

The UCDH workforce may not use public AI and/or public Generative AI (GenAI) tools for work purposes. Instead, UCDH has approved certain AI and GenAI tools for patient communication purposes, to enhance workflows, and to streamline updates to medical records. These approved tools have necessary safeguards in place to protect patient and institutional information.

PRIVACY SPOTLIGHT

Artificial Intelligence (AI) Tools

You can help keep UCDH patient and institutional information secure by:

- Only using versions of AI and GenAI tools approved by UCDH, not UCD Campus, public, or another/personal version.
- All UCDH users need to sign a User Agreement and comply with UCDH Administrative Policy **1350**, Generative AI Services and Application Use.
- Access to these tools is requested through the IT Self-Service system.

Please also review **Guidelines for Using Generative Artificial Intelligence (AI)**.

Photos and Video Recording

Photos and videos taken of patients help UC Davis Health (UCDH) meet mission goals. But we need to be careful when doing so because they can put patients' privacy at risk.

Unless the photos and/or videos are for treatment or only training within UCDH, **always get prior written permission from the involved patient to 1) take the photo, and 2) before use/sharing.**

More information is available by reviewing UC Davis Health policy **1426**, Authorization and Consent to Photograph or Interview.

Photos and Video Recording

Upload photos of treatment to the patient's electronic medical record (EMR) as necessary. Photos and/or videos taken for other work purposes should be stored in a UCDH-approved location, like OneDrive or SharePoint.

Only use Haiku and Canto apps for treatment photos. You are not allowed to use device manufacturer or purchased smartphone camera apps on personal devices to take or store photos and/or videos.

Promptly delete photos and/or videos from device(s) after adding them to the EMR or the UCDH-approved storage location.

For more information, please review UCDH **policy 2393** Creating, Using, and Managing Images in the Medical Setting and its attachments.

Social Media

Social media is great for sharing ideas and connecting with others, but if patient information is involved social media presents a risk to privacy.

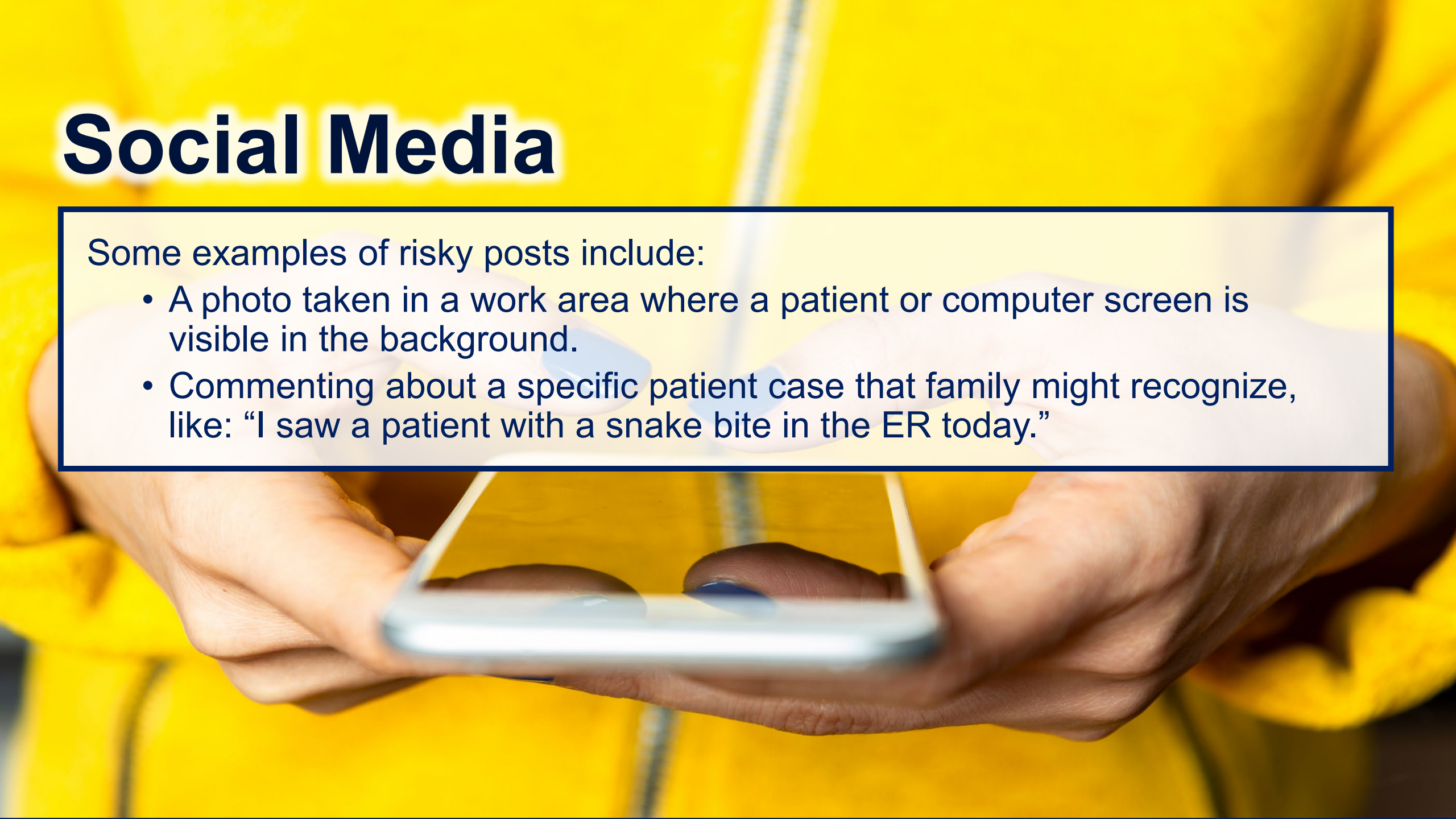
UC Davis Health (UCDH) **policy 1307** presents the rules for using social media. **These rules apply to everyone, whether posting on personal accounts, managing official UCDH accounts, or commenting on other sites**.

You cannot share patient information on social media without first getting written permission from the patient. Even then, posting should remain respectful and align with UCD's **Principles of Community**.

Social Media

Some examples of risky posts include:

- A photo taken in a work area where a patient or computer screen is visible in the background.
- Commenting about a specific patient case that family might recognize, like: “I saw a patient with a snake bite in the ER today.”



Social Media

Be extremely careful when posting about your work on social media. Here are some important rules for using social media:

- Do not share confidential information about the University.
- Do not use the University's name to suggest that your opinions are official.
- Do not mention UC Davis Health or its trademarks on your personal accounts.
- Never share any patient information on social media without their prior written permission.
- UC Davis Health does not encourage "friending" or following patients, and the workforce should only do this in certain situations (e.g., friendship before working at UCDH).

Social Media

Additional social media resources are available in the **UC Davis Health Social Media Toolkit** and UC Davis Health policy **1426**, Authorization and Consent to Photograph or Interview.

Confidential Patients

Some patients that present for care are in unique situations that require protecting their identity. A patient or someone else authorized to do so may request Confidential status and if approved it is granted to protect the use or disclosure of the patient's information.

For more information, please review UCDH policy **1190** Patient Placed on Confidential Status.

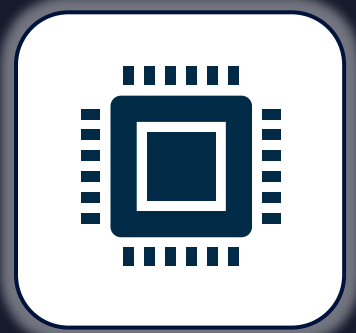
Privacy and Security Safeguards

Privacy and Security Safeguards

Click each image below to learn more about the safeguards UC Davis Health uses to protect patient information.

Administrative Safeguards

Physical Safeguards



Technological Safeguards

Administrative Safeguards

These are policies, procedures, written agreements, and workflows to help protect the privacy and security of patient information.

Some examples of administrative safeguards include:

- Annual privacy and security training for all workforce members
- Processes to handle privacy concerns and complaints
- Sanctions for breaking privacy laws, rules, and/or policies

Sections **2400** and **3500** of UC Davis Health's Administrative Policies Manual provide detailed guidance on safeguarding patient information.

Physical Safeguards

These include, but are not limited to:

- No printing from home/remote locations unless prior approval obtained.
- Locking documents and files in cabinets both in the office or at home/remote locations.
- Using keys, badges, and/or other systems to control access to buildings and work areas.
- Destroying documents and other items – like medication containers – when no longer needed.

Physical security tips:

- Do not leave doors open or unlocked if they are supposed to be locked.
- Be aware of potential unauthorized people in work areas, especially restricted ones.
- Never share your access codes, badges, or keys with anyone.
- Always maintain positive control of documents and mobile devices.

PRIVACY SPOTLIGHT

Physical Safeguards: Disposal

Patient Information must be disposed of in a manner that protects confidentiality and complies with HIPAA regulations.

At UC Davis Health, properly destroy documents and other physical items containing patient information by using the shred bins located throughout the institution. Printing from home is prohibited unless your management approves!

Any medication or other items that have patient information on them should be adequately covered or otherwise defaced to prevent readability or reidentification.

For electronic devices containing patient information, Information Technology should be contacted for assistance with disposal at (916) 734-4357.

Contact Environmental Health and Safety at **hs-safety@ucdavis.edu** or 916-734-3355 for support with shred bins or questions with regulated waste.

PRIVACY SPOTLIGHT

Physical Safeguards: Devices

Most large data breaches happen because of stolen or lost devices that aren't encrypted or lack encryption. These devices may include:

- Computers/laptops
- USB drives or portable hard drives
- Smartphones and tablets

Security Tips

- Always physically (and technically) secure these items, especially portable ones.
- Immediately report lost or stolen devices to your management and Information Technology (IT) by calling 916-734-4357.
- If the device stores patient information, also report it to Compliance and Privacy Services at privacyprogram@health.ucdavis.edu or 916-734-8808.

Technological Safeguards

Technological safeguards protect patient information by managing access and ensuring privacy. Some examples include:

- Encryption
- Passwords
- Anti-malware
- Access management
- Monitoring tools

Devices that do not meet these standards will be prevented from connecting to the UCDH network.

Information Technology (IT) regularly monitors all systems and records to make sure patient and institutional information is properly accessed, used, and shared.

Technological Safeguards

Protecting patient information is everyone's job. While the IT team handles many security tasks, you also play a key role. For more information, please review **Cyber Security | UC Davis Health,**

Tips to keep patient information safe

- Follow security best practices and University policies.
- Stay alert and be aware!
- Report any known or suspected security or privacy issues right away.

Avoid Unnecessary Risks

- Custom and/or personal databases and devices can be risky if not properly secured.
- Systems not managed by IT might lack proper controls.
- Do not use any unapproved web applications, software, or technology.
- Remember that you are the key to ensuring a secure environment that protects our patient and institutional information

Act

- Let IT know about custom technology you use so they can help you to properly protect it.

PRIVACY SPOTLIGHT

Technological Safeguards: Risk Assessment

A Risk Assessment must be performed prior to any activation or use of Technology at UC Davis Health. Technology may include web applications, software, and other tools/resources.

- Cybersecurity and IT perform the risk assessment and IT issues an Authority to Operate (ATO) new technology.
- This is necessary to protect patient and institutional information, meet regulatory requirements, and comply with University and UCDH Administrative Policy.
- Getting in the IT “frontdoor”: Request New Technology Initiatives.

PRIVACY SPOTLIGHT

Technological Safeguards: Devices

UC Davis Health is a “bring-your-own-device” (BYOD) institution. If you choose to use your personal device for UCDH business, please enroll it in the **BYOD Program**! The Program uses an IT-approved tool to help with separating your personal data from your work data. The Tool does not allow UCDH to access your personal data.

To use your device for UCDH business, you need to:

- Secure it with a PIN or biometric login.
- Backup data and encrypt the backups.
- Enable device locating services (e.g., Find My Device).

PRIVACY SPOTLIGHT

Technological Safeguards: Devices

Important points:

- Any work information stored on your device is owned by the University of California. Best practice is to not store items on the device but in UCDH-approved storage locations and apps. Please contact the UCDH IT Helpdesk for support.
- There is no reasonable expectation of privacy on any device you use for University of California business.
- Not properly protecting confidential information stored on your device can lead to disciplinary action, including termination. Please review UC Davis Health policy **1010**, Policy Enforcement, for more information.

For more details, please review UC Davis Health policy **1313**, Protected Health Information or Personal Information on Mobile Devices and Personal Computers

PRIVACY SPOTLIGHT

Technological Safeguards: Passwords/Passphrases

Password/Passphrase Tips

- Use a passphrase when possible.
- Passphrases should have at least 15 characters, including upper case, lower case, numbers, and special characters.
- Avoid easy-to-guess passwords/passphrases like birthdays, pet names, or repetitive characters (e.g., 1111, aaaaa).
- Don't use the same password/passphrase for multiple accounts!
- Don’t use passwords/passphrases involved in a breach.
- Use an IT provided Password Manager, like Lastpass, to securely generate and store passwords.

Examples:

- Good passphrase: I’m the world’s #1 doctor
- Bad password: fluffy1234

PRIVACY SPOTLIGHT

Technological Safeguards: Passwords/Passphrases

More Password Tips

- Use different passwords for personal and work systems.
- Never share your passwords with anyone.
- Change passwords regularly and do not write them down, especially where others can see them. Best practice is to not change passphrases
- If you think your password is compromised, change it immediately and call the UC Davis Health Technology Operations Center (TOC) at 916-734-4357.

For more information, please review UCDH policy **1301-0012**, Password and Passphrase Standard. See also **Attachment A** in UCD policy 310-22, UC Davis Security Standards.

PRIVACY SPOTLIGHT

Technological Safeguards: Threats

Malware

- Malware is harmful programs that can damage/disrupt your computer or steal data. This threat often comes from foreign nation states or organized crime groups.*
- The most common types impacting UC are*:
  - Ransomware: encrypts data and demands payment for the decryption key so you can access the data.
  - Spyware: Secretly collects patient, personal, or institutional information; or shows unwanted content.

One malware infection can negatively impact health system operations, data, and patient care. IT manages advanced malware detection software on IT managed computers and mobile devices. If you are using a personal device, please enroll it in the IT **BYOD** program to ensure it is properly protected from malware and other threats.

*Source: UC threat briefing from Google Mandiant

PRIVACY SPOTLIGHT

Technological Safeguards: Threats

Internet Threats

The internet is filled with web sites and software that may contain malware.

Here are some tips to stay safe online:

- Do not assume a link is safe because it appears in the search results on a reputable search engine site (e.g., Google, Bing). Attackers often spread malware using “sponsored” links returned in search results. Sponsored links are blocked by UCDH IT.
- If your web browser alerts you that something is wrong, do not ignore it! Navigate away from the search result/website right away.
- Think before you click and use good judgement

PRIVACY SPOTLIGHT

Technological Safeguards: Electronic Communications

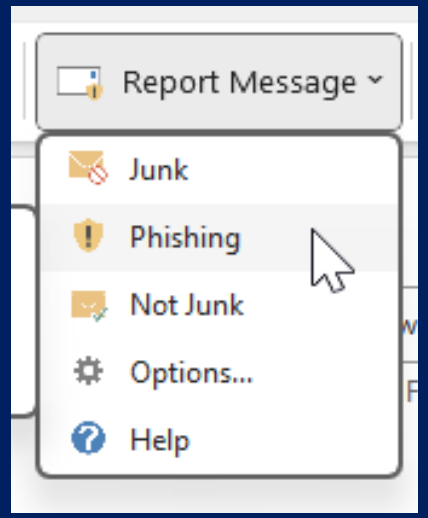
Email

Email is a tool we use everyday for work, and so do criminals to:

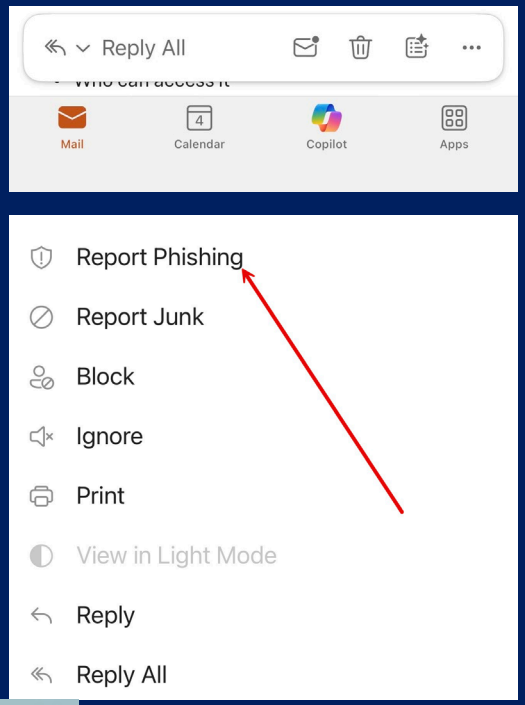
- Deliver malware
- Phish people ("You won $650,000 in the lottery. Contact Jane Doe with your details in the next 24 hours to claim your prize.")

Do not open attachments, click on a link, or reply to suspicious or spam e-mails. If you did not expect the email and/or attachment or it seems suspicious, report the event by using the Report Phishing button in Outlook, as presented to the right.

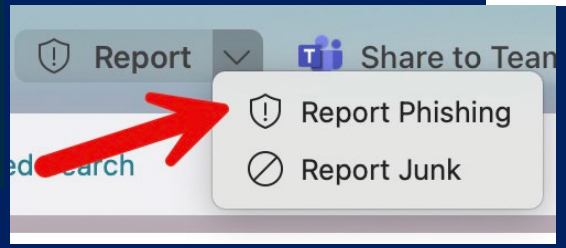
Windows



iPhone



Mac



PRIVACY SPOTLIGHT

Technological Safeguards: Electronic Communications

Secure Messaging Tips

- Only use your assigned Outlook email account (@health.ucdavis.edu) to send UCDH business emails.
- If sending an email to a non-UC Davis Health email account, encrypt it by typing #secure# in the subject line or body, or using the “encrypt” function in the email’s “options” ribbon.
- Use MyChart to communicate with patients because it is a secure tool best setup for this work purpose.
- Use Physician Connect to communicate with non-UC Davis Health medical professionals about the care of mutual patients because it is a secure tool best setup for this work purpose.

For more information, see, UC Davis Health policies 2442, Email Communication that Contains Protected Health Information or Personal Information, and 1314, E-Mail Use for UCDH Personnel.

PRIVACY SPOTLIGHT

Technological Safeguards: Surveillance

UC Davis Health monitors access to electronic records:

- Your activity in Epic and other electronic systems is logged and monitored.
- Advanced technology detects suspicious access.
- Compliance and Privacy Services reviews and investigates identified instances of potential unauthorized access.

Consequences:

- Inappropriately accessing or sharing patient information can lead to disciplinary action, including being terminated from employment and reported to law enforcement agencies. Please review UC Davis Health policy 1010, Policy Enforcement, for more information.

For more information, please review UCDH policy 2448, Privacy and Surveillance Program.

Why are privacy and security so important?

Protecting privacy is the right thing to do.

The public trusts UC Davis Health with protecting the information given to us. We also have a moral and ethical responsibility to safeguard this information as though it were our own, or that of our loved ones.

For more information, please review the University of California Statement of Ethical Values.

Privacy violations can harm people

Identity theft can start small:
Sharing a patient's name and where they were treated can lead to identity theft. Social engineering happens!

For example:
If someone knows a patient's name and treatment location, they could pretend to be that person, call a UC Davis Health helpdesk for support, and possibly get access to a patient’s itemized mailed billing information or their MyChart account.

Privacy violations can result in steep fines and penalties for UC Davis Health and **YOU**.

UC Davis Health must **immediately report** any unlawful or unauthorized access to, or use or sharing of, a patient's information. For more information, please review UCDH **policy 1302**, Protected Health Information, Personal Information Breach Notification.

STATE LAW
Must report breaches to the California Department of Public Health within 15 business days of detection.

FEDERAL LAW
Must report breaches of patient information to U.S. Health and Human Services within 60 calendar days of discovery.

PATIENT NOTIFICATION
Must be reported to affected patients as well.

Privacy violations can result in steep fines and penalties.

Violations may result in fines and penalties against UC Davis Health and individuals. Examples of civil monetary penalties (CMP) for violating HIPAA:

Tiers	Violation Type	Minimum Penalty	Maximum Penalty per Violation	Annual Cap per Identical Violation
Tier 1	The covered entity did not know and could not reasonably have known of the violation	$137	$68,928	$2,067,813
Tier 2	The violation was due to reasonable cause and not willful neglect	$1,379	$68,928	$2,067,813
Tier 3	The violation was due to willful neglect, but corrected within the required time	$13,785	$68,928	$2,067,813
Tier 4	The violation was due to willful neglect and not corrected	$68,928	$2,067,813	$2,067,813

Privacy violations can result in steep fines and penalties.

Violations may result in fines and penalties against UC Davis Health and individuals. Examples of criminal penalties for violating HIPAA:

Tiers	Violation Type	Criminal Penalty
Tier 1	Knowingly obtaining or disclosing PHI	Up to $50,000 fine and up to 1 year in prison
Tier 2	Offense committed under false pretenses (e.g., misrepresenting identity or purpose)	Up to $100,000 fine and up to 5 years in prison
Tier 3	Offense committed with intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm	Up to $250,000 fine and up to 10 years in prison

Privacy violations can result in disciplinary action

In addition to possibly being fined, the access, use, or sharing of patient information without authorization or a work purpose may result in disciplinary action up to and including termination of employment. Please review UCDH **policy 1010**, Policy Enforcement. A referral to regulatory agencies and/or law enforcement may also occur.

What are my reporting responsibilities?

Any unauthorized access, use, or sharing of a patient's information must be immediately reported, as listed in UC Davis Health policy **1302**, Protected Health Information, Personal Information Breach Notification.

Some examples include, but are not limited to:

- A loss or theft of an electronic device
- Sharing of patient documentation or images to a wrong person
- An employee accessing patient information for a non-work purpose

Compliance and Privacy Services conducts all patient privacy-related investigations and determines whether and to whom a breach must be reported, and coordinates notification as required.

Protection from Retaliation

Open communication and the freedom to report concerns about UC Davis Health operations and/or ethics are essential to the Compliance Program's success.

Retaliation, retribution, and/or harassment of anyone who makes a good faith report about a known or suspected violation will not be tolerated.

UC policy, federal law, and state law also protects any whistleblower employee or applicant for employment for having reported an issue or filing a whistleblower report.

The UC Whistleblower Protection policy can be found online at **https://www.ucop.edu/uc-whistleblower/**.

Privacy and Security Summary

What patient information needs to be protected by law:

- Individually identifiable, PHI, medical, and PI.

Your role in keeping patient information private and secure:

- You must first get a patient's authorization to use, access, or share it for a work purpose if the law does not allow or require you to do so.
- Access, use, and share patient information only when needed to do your job.
- Job duties usually include TPO and may include other assigned purposes.
- Use only the minimum amount of patient information needed to do your job.
- Patients have many rights related to their information that we maintain

Privacy and Security Summary

Why protecting patient information is important:

- It builds trust with our community.
- Law and policy require us to do so.
- It’s the right thing to do.
- Privacy violations can hurt people.
- Failing to do so can have serious consequences for both UC Davis Health and you.

Questions?

Compliance and Privacy Services Department
Alhambra Cannery Building
1651 Alhambra Boulevard
Main line: (916)734-8808
Fax: (916)734-4179

UCDAVIS HEALTH

Compliance Hotline: (800) 403-4744
Privacy Help: privacyprogram@health.ucdavis.edu
General Compliance Help: compliancehelp@health.ucdavis.edu
Research Compliance Help: researchcompliance@health.ucdavis.edu
Web: https://health.ucdavis.edu/compliance/privacy/
Cyber Security: https://health.ucdavis.edu/cybersecurity/

End of Course

To receive credit for completing this training, you will need to read and agree to the following confidentiality statement.