



**LOS ANGELES COUNTY DEPARTMENT OF HEALTH SERVICES
HARBOR-UCLA MEDICAL CENTER**

SUBJECT: SAFEGUARDS FOR PROTECTED HEALTH INFORMATION (PHI) **POLICY NO.** 706

CATEGORY: Health Information Mgmt.	EFFECTIVE DATE: 4/03
POLICY CONTACT: Charles Onunkwo, Keisha Belmaster	UPDATE/REVISION DATE: 2/22
REVIEWED BY COMMITTEE(S):	

PURPOSE:

To establish safeguards to protect the security of Protected Health Information (PHI) and other confidential information from unauthorized viewing, acquisition, access, use, or disclosure.

POLICY:

Harbor-UCLA Medical Center's workforce must reasonably safeguard PHI to limit incidental access, use, or disclosures made pursuant to an otherwise permitted or required use or disclosure.

DEFINITIONS:

Desktop Workstation: Includes a stand-alone, generally stationary, personal computing device possibly connected to a network server or other computer.

Particularly Sensitive Health Information: Protected Health Information that is generally considered highly confidential including, but not limited to, mental health, drug and alcohol abuse, and communicable disease information.

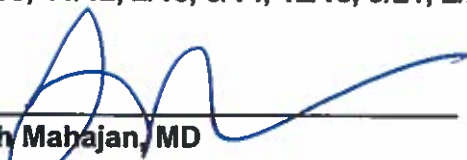
Portable Computing Devices: Includes, but is not limited to, the following:


- Portable computers, including, but not limited to, laptops and tablet computers.
- Portable devices, including, but not limited to, personal digital assistants (PDAs), digital cameras, smartphones, cellular telephones, and pagers.
- Portable storage media, including, but not limited to, diskettes, tapes, DVDs, CDs, USB flash drives, memory cards, and external hard disk drives.
- Mobile computers that can connect by cable, telephone wire, wireless transmission, or via any Internet connection to County Information Technology resources.

REVISED: 2/05, 2/13, 12/15, 9/21, 2/22

REVIEWED: 2/05, 12/08, 11/12, 2/13, 8/14, 12/15, 9/21, 2/22

APPROVED BY:


 Anish Mahajan, MD
 Chief Executive Officer
 Chief Medical Officer


 Griselda Gutierrez, MD
 Associate Chief Medical Officer


 Jason Black, MBA, DNP, RN
 Chief Nursing Officer



LOS ANGELES COUNTY DEPARTMENT OF HEALTH SERVICES
HARBOR-UCLA MEDICAL CENTER

SUBJECT: SAFEGUARDS FOR PROTECTED HEALTH INFORMATION (PHI) POLICY NO. 706

Protected Health Information (PHI): Individually identifiable information relating to past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present, or future payment for health care provided to an individual.

Workforce Member: A workforce member is either County or Non-County, and includes employees, contract staff, affiliates, volunteers, trainees, students, and other persons whose conduct, in the performance of work for the Department of Health Services, is under its direct control, whether or not they receive compensation from the County. Harbor-UCLA Medical Center, its offices, programs, or facilities, is under its direct control of Harbor-UCLA Medical Center, regardless of whether or not they receive compensation from the County.

PROCEDURE:

Harbor-UCLA Medical Center will implement appropriate administrative, technical, and physical safeguards that will reasonably safeguard Protected Health Information from any intentional or unintentional acquisition, viewing access, use, or disclosure that is in violation of privacy policies.

I. Administrative Safeguards

- A. **Oral Communications.** Harbor-UCLA Medical Center's workforce must exercise due care to avoid unnecessary disclosures of Protected Health Information through oral communications. Conversations in public areas should be avoided unless necessary to further patient care, research, or teaching purposes. Voices should be lowered and modulated, and attention should be paid to unauthorized listeners in order to avoid unnecessary disclosures of Protected Health Information. Patient identifying information only should be disclosed during oral conversations when necessary for further treatment, payment, teaching, research, or operational purposes. Dictation and telephone conversations should be conducted away from public areas if possible. Speakerphones only should be used in private areas and attention must be paid to the sound level.
- B. **Cellular Telephones.** The use of cellular phones is not prohibited as a means of disclosing or using PHI. However, their use poses a higher risk of interception as compared to legacy landline telephones. Landline telephones should be used if the conversation will involve the disclosure of PHI.
- C. **Telephone Communications.** Harbor-UCLA Medical Center must exercise protocols consistent with DHS guidelines to protect the confidentiality and privacy of patient information when communicating via telephone. Whenever it is necessary for workforce members to discuss PHI via telephone with a patient or patient's family members, business associates, or other health care providers, workforce members must follow facility guidelines for protecting such information. Release of information over the phone may only be done if the person doing so is absolutely sure of the identity of the person s/he is speaking with and that person has the right to receive the information.

Harbor-UCLA Medical Center's workforce members will honor any agreement made with the patient or patient's personal representative regarding alternate forms of communications or restrictions on the use or disclosure of the patient's PHI. Telephone communications involving PHI should be conducted in a private area whenever possible and in a low voice to ensure information is not overheard by unauthorized persons. When receiving calls, workforce members shall not discuss PHI with the caller until the following can be confirmed:



LOS ANGELES COUNTY DEPARTMENT OF HEALTH SERVICES
HARBOR-UCLA MEDICAL CENTER

SUBJECT: SAFEGUARDS FOR PROTECTED HEALTH INFORMATION (PHI) **POLICY NO.** 706

1. Identity of the caller (e.g., a "call back" to validate the number called, or definite voice recognition).
 2. Verification that the caller has a need to know, and the use and disclosure of PHI is permissible.
- D. **Internet Communications.** If a patient requests receipt of their PHI through the Internet, the workforce member must ensure the information is encrypted. If the information cannot be encrypted, the information must be sent through an alternate secure means of communication.
- E. **Telephone Messages.** When making calls, workforce members shall not discuss PHI until the identity of the person on the phone line has been confirmed. In the event an answering machine or voice mail system picks up the call, staff should leave a message requesting that the person they need to speak to return the call.
1. The message shall include ONLY the name and telephone number of the person that should receive the return call (e.g., "This message is for Mary Jones. Please contact Mary Smith at 555-1313).
 2. Messages left on an automatic answering machine or voice mail system shall not contain PHI (e.g., diagnosis, test results, etc.).
 3. Telephone messages and appointment reminders may be left on answering machines and voice mail systems unless the patient has requested an alternative means of communication pursuant to **DHS Policy No. 361.6, "Right to Request Confidential Communications of Protected Health Information"**. However, each provider and/or clinic should limit the amount of Protected Health Information that is disclosed in a telephone message.
 4. The content of appointment reminders should not reveal particularly sensitive health information, directly or indirectly, such as the specific name of the unit/department of the hospital.
 5. Telephone messages regarding test results or that contain information that links a patient's name to a particular medical condition should be avoided.
- F. **Faxes.** The following procedures must be followed when faxing PHI:
1. Only the PHI necessary to meet the requester's needs should be faxed.
 2. Particularly sensitive health information should not be transmitted by fax except in emergency situations or if required by a government agency. If particularly sensitive health information must be faxed, the recipient should be notified immediately prior to the transmission and the sender should immediately confirm that the transmission was completed, if possible.
 3. Harbor-UCLA Medical Center workforce members should only fax PHI authorized as part of their work duties.
 4. Unless otherwise permitted or required by law, a properly completed and signed authorization must be obtained prior to releasing Protected Health Information to third parties for purposes other than treatment, payment, or health care operations as provided in **DHS Policy No. 361.4, "Use and Disclosure of Protected Health Information (PHI) Requiring Authorization"** unless otherwise permitted or required by law. In certain instances, an authorization may be needed to release information to a third party for payment, such as self-paid services, or insurance purposes.
 5. Protected Health Information may be faxed to an individual if the individual requests access to their own PHI in accordance with **DHS Policy 361.15 "Access of Individuals to Protected Health Information (PHI)/Designated Record Set"**.



LOS ANGELES COUNTY DEPARTMENT OF HEALTH SERVICES
HARBOR-UCLA MEDICAL CENTER

SUBJECT: SAFEGUARDS FOR PROTECTED HEALTH INFORMATION (PHI) **POLICY NO.** 706

6. All faxes containing Protected Health Information must be accompanied by a cover sheet that includes a confidentiality statement. Use Harbor-UCLA Medical Center's ***PHI FAX Form (ATTACHMENT I)***.
7. Reasonable efforts should be made to ensure that fax transmissions are sent to the correct destination. Frequently used numbers should be preprogrammed into fax machines or computers to avoid misdialing errors. Preprogrammed numbers should be verified on a routine basis. The numbers of new recipients should be verified prior to transmission.
8. Fax machines must be located in secure areas not readily accessible to visitors and patients. Incoming faxes containing Protected Health Information should not be left sitting on or near the machine.
9. Approved DHS fax confirmation sheets should be reviewed to ensure the intended destination matches the number on the confirmation. The confirmation sheet should be attached to the document that was faxed. Verify receipt of the fax by contacting the intended recipient and noting such on the approved fax sheet.
10. Misdirected faxes containing Protected Health Information should be investigated and reported to the supervisor and the Facility Privacy Officer. The sender should make an attempt to call the recipient to retrieve the misdirected fax, if possible. Do not read through faxes received in error; contact the sender and advise that their fax was received in error and properly destroy the information.

G. Mail.

1. **Interoffice Mail:** Use a sealed envelope (not one with holes in it) and properly address the envelope with the name of the recipient as well as the location and room number. Tape the opening and write or stamp "Confidential" over the seal.
2. **Outside Mail:** Use an appropriate sealed envelope for U.S. Mail. Ensure the return address does not contain the name of the department or unit within the hospital to ensure added privacy.

H. Internet/Social Networking.

Internet/social networking sites must not be used to discuss patients or patient information. Workforce members must remember that although internet/social networking sites (e.g., Twitter, Facebook, YouTube, discussion forums, text messaging, web mail, etc.) can be accessed on their own time from their own computing devices, they should remember that due to the nature of the work and the type of business they work in, just small bits of information, put together, can reveal identifying information about patients and cause them to violate privacy laws.

1. Workforce members must not disclose any confidential or proprietary information of or about the County, DHS, or any of our affiliates on social networking sites.
2. Workforce members must not hold themselves out as representatives of the County or DHS or act on behalf of the County of DHS on social networking sites, unless specifically authorized in writing.
3. Workforce members, including former workforce members, may be held liable for damages and potential criminal prosecution for breaching PHI used or exposed to while working for Harbor-UCLA Medical Center.
4. Workforce members must not engage in internet/social networking activities on their personal computing device during County work hours.



LOS ANGELES COUNTY DEPARTMENT OF HEALTH SERVICES
HARBOR-UCLA MEDICAL CENTER

SUBJECT: SAFEGUARDS FOR PROTECTED HEALTH INFORMATION (PHI) POLICY NO. 706

- I. **Photographing and Recording Patients.** Photographic or audio recordings of a patient may be taken for purposes of treatment, professional education, peer review, publication, research, law enforcement, public relations, marketing, and news media only upon obtaining prior written patient consent and photographs must be filed in the patient's medical record. Disclosure of photographic or audio recordings constitutes the release of medical information and therefore requires prior authorization for the use or disclosure of protected health information.
 1. Written patient authorization must be obtained prior to taking photographs, video, or recordings of patients (See Attachment II – Consent to Photograph and Authorization for Use or Disclosure (English), Attachment III (Spanish)).
 2. Authorization must contain the specific reason and use. Any other or additional use or disclosure requires a new authorization.
 3. Only facility-owned cameras, memory cards, and other equipment may be used.
 4. A workforce member's use of personal photography or recording equipment (including cellular telephones and smartphones) is prohibited.
 5. Photography of medical records or any other documentation that contains PHI is strictly prohibited.
 6. DHS Policy 304 provides guidelines for photographing and recording patients.

- J. **Destruction Standards.** Protected Health Information must be discarded in a manner that protects the confidentiality of such information. Paper and other printed materials containing Protected Health Information should be shredded or placed in the locked shredder bin instead of throwing them in the trash. Contact your IT/Help Desk to appropriately destroy electronic Protected Health Information located on electronic media (e.g. CDs, USB thumb drives, hard drives, computer/laptops, etc.).
 1. PHI awaiting disposal or destruction must be stored in secure containers, storage rooms, or centralized shredder bins that are appropriately labeled and are properly disposed of on a regular basis. Reasonable steps must be taken to minimize access to those documents.
 2. Storage rooms containing confidential information awaiting disposal must be locked after business hours or when authorized staff is not present.
 3. Centralized bins or containers used for disposal of confidential information must be sealed, clearly labeled "Confidential", "PHI" or some other suitable term, and placed in a secure location. Reasonable steps must be taken to minimize access to PHI.
 4. Documents containing PHI must not be recycled or reused for scratch paper.
 5. A certified County approved vendor will be responsible for the removal and disposal of the PHI waste bins throughout the facility. As a backup plan, shredder bins that are full should be reported to Environmental-Housekeeping Department at (424) 306-8370 for additional pick-up.
 6. Portable media awaiting destruction/sanitization must be kept in a secure locked area.

II. **Physical Safeguards**

- A. **Paper Records.** Paper records and medical charts must be stored or filed in such a way as to avoid access by unauthorized persons. Some type of physical barrier should be used to protect paper records from unauthorized access.
 1. Paper records and medical charts on desks, counters, or nurses' stations must be placed face down or concealed to avoid access by unauthorized persons.



**LOS ANGELES COUNTY DEPARTMENT OF HEALTH SERVICES
HARBOR-UCLA MEDICAL CENTER**

SUBJECT: SAFEGUARDS FOR PROTECTED HEALTH INFORMATION (PHI) POLICY NO. 706

2. Paper records should be secured when the office is unattended by persons authorized to have access to paper records.
3. Original paper records and medical charts should not be removed from the premises unless permitted by law and they are secured in a manner to protect the PHI and are not to be left unattended.
4. Do not store paper records in an area where they can be thrown away or mistaken for trash.

B. Physical Access

1. Persons authorized to enter areas where Protected Health Information is stored or viewed must wear an identifiable Harbor-UCLA Medical Center employee badge or be escorted by an authorized workforce member.
2. Persons attempting to enter an area where Protected Health Information is processed must have prior authorization by Harbor-UCLA Medical Center management.
3. Workforce members must not allow others to use or share their badges or keycards and must verify access authorization for unknown people entering an area where Protected Health Information is stored or processed.

C. Visitors and Patients

To ensure visitors, vendors, and patients do not access Protected Health Information, they must be appropriately monitored. This means that persons that are not part of Harbor-UCLA Medical Center's workforce should not be in areas in which patients are being seen or treated or where Protected Health Information is stored without appropriate supervision.

D. Desktop Workstations

Protected Health Information on computer devices must be protected from unauthorized viewing and unauthorized access. Suggested means for ensuring this protection include:

1. Using polarized screens or other computer screen overlay devices that shield information on the screen;
2. Placement of computers out of the visual range of persons other than the authorized users;
3. Clearing information from the screen when not being used;
4. Using password-protected screen savers when computer workstations are not in use; and
5. Locating computers in areas that prohibit/restrict access by unauthorized individuals (e.g. not within reach of persons at the counter, etc.).

E. Remote Access or Working Offsite/Outside the Secure Work Environment

Harbor-UCLA Medical Center's workforce members are discouraged from removing Protected Health Information from the facility; however, it is recognized that there are some situations where work outside of the secured environment is necessary. When it is necessary for Harbor-UCLA Medical Center staff to take patient information home or to another work environment, the following guidelines in accordance with **DHS Policy 935.11, "Workstation and Mobile Device Use & Security Policy"** should be used:

1. The remote work area must provide adequate privacy and security.
2. Confidential information should be secured in locked rooms or a locked storage container when not in use.
3. Home computers must comply with DHS standards including County approved anti-virus software and must adhere to County hardware/software protection standards and procedures.



**LOS ANGELES COUNTY DEPARTMENT OF HEALTH SERVICES
HARBOR-UCLA MEDICAL CENTER**

SUBJECT: SAFEGUARDS FOR PROTECTED HEALTH INFORMATION (PHI) **POLICY NO.** 706

4. While on the train, bus, airplane, or another form of mass transit ensure the use of a privacy screen as well as all other requirements under Section V – Desktop Workstations. Paper documents must be kept out of sight or range of view by other passengers.
5. Confidential data may not be saved on removable devices (e.g., floppy drive, CD-ROM, external drive, USB/Thumb drive) unless it is approved and appropriate safeguards are in place (e.g., encryption).
6. Data/information must not be accessible by unauthorized persons/family members. All completed work, if not remotely accessed, must be saved to the original, encrypted external device AND removed completely from the home computer.
7. External devices, portable computing devices, must be encrypted and maintained in a secure location/protected from theft or loss.

III. Technical Safeguards

Access to Protected Health Information is based on the role and job responsibilities of the workforce member. Workforce members will be assigned access to Harbor-UCLA Medical Center's networks and systems based on their need to know and the minimum amount of information needed to fulfill their job responsibilities. Minimum necessary also applies to their access to the system. A workforce member with access to a system for completion of certain assignments is not authorized to view, use or access other information in the system not related to their job responsibilities.

A. Technical safeguards regarding the protection of Protected Health Information maintained in electronic form may include:

1. Log off any electronic system containing PHI when leaving the computer, even for a few minutes, or after obtaining necessary data.
2. Require computing devices to have a password-protected screen saver or other time-out feature.
3. All portable computing devices such as laptops, USB/thumb drives, and other electronic devices containing Protected Health Information.
4. Workforce members should be familiar with their facility's downtime procedures.

B. Passwords:

1. Workforce members are responsible for safeguarding their passwords for access to the County's information technology resources.
2. Workforce members are responsible for all transactions made using their passwords.
3. Workforce members may not provide their password or use their password to provide access to another workforce member or access the County information technology resource with another workforce member's password or account. Some systems have a universal access password with a secondary password neither of which shall be shared with workforce members who are not authorized to utilize the system.
4. Passwords must be changed on a regular basis to ensure security. Strong passwords include at least eight characters, such as a combination of letters, numbers, and/or special characters.
5. Ensure all areas used to store PHI are properly secured and that only authorized personnel have access to those locations.

IV. Use of Electronic Systems



LOS ANGELES COUNTY DEPARTMENT OF HEALTH SERVICES
HARBOR-UCLA MEDICAL CENTER

SUBJECT: SAFEGUARDS FOR PROTECTED HEALTH INFORMATION (PHI)

POLICY NO. 706

Harbor-UCLA Medical Center shall implement a combination of administrative, physical, and technical safeguards to protect PHI in electronic communications networks, including (1) privacy and security awareness training of Harbor-UCLA Medical Center Users concerning the transmission of PHI over electronic communications networks; (2) periodic review of this policy and procedure Harbor-UCLA Medical Center Users to confirm compliance; (3) repeated security reminders; (4) use of password-protected screen savers and exercise of due diligence to ensure that electronic systems used for transmission and/or storage of PHI is protected from viewing by unauthorized persons; (5) other applicable safeguards outlined in this Policy.

A. Portable Computing Devices

1. All portable computing devices that access and/or store PHI or confidential information must comply with all applicable DHS and County IT resources policies, standards, and procedures.
2. Generally, DHS prohibits the download or storage of PHI and/or confidential information on portable computing devices. However, Harbor-UCLA Medical Center Users who, in the course of County business, must download or store PHI and/or confidential information on portable computing devices are required to adhere to DHS policies and procedures for storage and use of PHI and/or confidential information on portable computing devices.
3. If PHI and/or confidential information is downloaded or stored on a portable computing device, information must be protected from unauthorized access, and, without exception, the information must be encrypted.
4. A DHS User who intends to use their County-owned or personally owned portable computing device to access and/or store PHI and/or confidential information is required to obtain prior written authorization from Harbor-UCLA Medical Center Information Technology.

B. Personal Digital Assistants (PDAs)

1. All PDA users will be provided specific training on the risks of using PDAs for PHI and will be required to recertify their understanding and compliance with HIPAA privacy policies and procedures.
2. PDAs, whether procured by Harbor-UCLA Medical Center or personally owned, will be permitted for PHI use but must be registered with the DHS CISO (Cluster Information Security Coordinator) or designee and must conform to departmental standards for password protection.

C. E-Mail

1. Non-County e-mail such as G-Mail, Yahoo Mail, etc. must not be used for sending Harbor-UCLA Medical Center-related Protected Health Information. Use of e-mail between a Harbor-UCLA Medical Center User and a patient is permitted provided that the e-mail is encrypted and sent through the County's e-mail system.
2. Harbor-UCLA Medical Center users must follow the same procedures when replying to e-mails with patient, confidential, and/or sensitive information in the same manner as if it were originally created by the Harbor-UCLA Medical Center user.
3. Auto-forwarding e-mails to any non-County e-mail account is strictly prohibited.
4. Audits of outbound e-mail communications may be periodically performed to ensure that the use of e-mail to transmit Protected Health Information is in accordance with Departmental policies. Refer to DHS Policy 935.20, "Acceptable Use Policy for County Information Technology Resources".



LOS ANGELES COUNTY DEPARTMENT OF HEALTH SERVICES
HARBOR-UCLA MEDICAL CENTER

SUBJECT: SAFEGUARDS FOR PROTECTED HEALTH INFORMATION (PHI)

POLICY NO. 706

D. Wireless Local Area Networks (WLANs)

1. WLANs that currently implement or have plans to implement WLAN security as defined by the DHS Network Security Architecture and County guidelines for Wireless Network Security are permitted for PHI use but must have a WLAN topology and security plan submitted and approved by the DHS CISO or designee.
2. WLANs that do not meet or plan to meet WLAN security guidelines as defined by the DHS Network Security Architecture and County guidelines for Wireless Network Security are not permitted and must be removed from service.

E. Electronic Transmission of Clinical Laboratory Tests

1. The health care professional must obtain a California-compliant authorization from the patient for the patient to receive his or her laboratory results by Internet posting or other electronic means. (Cal. Health & Safety Code § 123148(b)(1)). A patient (or his or her physician) may revoke this authorization at any time and without penalty, except to the extent that action has been taken in reliance on the authorization.
2. The transmission of the following clinical laboratory test results (and any other related results) to a patient by Internet posting or other electronic means is prohibited by law:
(i) HIV antibody test; (ii) presence of hepatitis antigens; (iii) drug abuse; and (iv) test results related to routinely processed tissues, including skin biopsies, Pap smear tests, products of conception, and bone marrow aspirations for morphological evaluation, if they reveal a malignancy.
3. In the event that a health care professional arranges for the electronic transmission of test results, the results must be delivered to the patient in a reasonable time period, but only after the results have been reviewed by the health care professional. When clinical laboratory test results are delivered to a patient via Internet posting or other electronic manner, access must be restricted by the use of a secure personal identification number.
4. If the patient asks to receive his or her laboratory test results by Internet posting, the health care professional is required to inform the patient of any charges that may be incurred directly to the patient or insurer for the service and that the patient may call the health care professional for a more detailed explanation of the laboratory test results when delivered.

F. Online Web-based Document Sharing Services

Storing and/or sharing of PHI and other confidential information using non-County approved online web-based document sharing services (e.g., Google Docs, Microsoft Office Live, Open Office, Dropbox, etc.) is strictly prohibited.

V. Disciplinary Action

Unauthorized viewing, acquisition, access, use, or disclosure of confidential and/or Protected Health Information (including but not limited to medical records) will result in disciplinary action, up to and including discharge, as well as possible civil/criminal penalties, fines and disciplinary action against the individual's professional license, permit, registration, or certificate from the issuing board or agency.

VI. Document Retention

This policy will be retained for a period of at least 6 years from the date of its creation or the date when it was last in effect, whichever is later.

REFERENCES:

45 Code of Federal Regulations, Part 164 Section 164.530 (c)(1)



**LOS ANGELES COUNTY DEPARTMENT OF HEALTH SERVICES
HARBOR-UCLA MEDICAL CENTER**

SUBJECT: SAFEGUARDS FOR PROTECTED HEALTH INFORMATION (PHI)

POLICY NO. 706

DHS Policy Numbers:

- 361.6 Right to Request Confidential Communications of Protected Health Information
- 361.4 Use and Disclosure of Protected Health Information (PHI) Requiring Authorization
- 361.15 Access of Individuals to Protected Health Information (PHI)/Designated Record Set
- 361.26 Mitigation
- 935.043 Blackberry Handheld Devices for Remote GroupWise Access Policy
- 935.11 Workstation & Mobile Device Use and Security Policy
- 935.20 Acceptable Use Policy for County Information Technology Resources

DHS Discipline Manual and Guidelines



Harbor-UCLA
MEDICAL CENTER

Los Angeles County
Board of Supervisors

Hilda L. Solis
First District

Holly J. Mitchell
Second District

Sheila Kuehl
Third District

Janice Hahn
Fourth District

Kathryn Barger
Fifth District

Anish Mahajan, MD, MS, MPH
Chief Executive Officer
Chief Medical Officer

Griselda Gutierrez, MD
Associate Chief Medical Officer

Jason Black, MBA, DNP, RN
Chief Nursing Officer

Azar Kattan
Chief Operations Officer

1000 West Carson Street
Torrance, CA 90509

Tel: (XXX) XXX-XXXX
Fax: (XXX) XXX-XXXX

ATTACHMENT I

F A X C O V E R S H E E T

Date: _____

Number of pages including Cover Sheet: _____

To: _____

Fax: _____

Phone: _____

Re: _____

From: _____

Fax: _____

Phone: _____

Urgent **For Review** **Please** **Comment** **Please Reply**

Comments:

To put patients first and provide exceptional patient-centered care with the compassion and respect we would want for our loved ones, regardless of the ability to pay.

The information contained in this facsimile is privileged and confidential and is intended only for the use of the recipient listed above. If you are neither the intended recipient or the employee or agent of the intended recipient responsible for the delivery of this information, you are hereby notified that the disclosure, copying, use or distribution of this information is strictly prohibited. If you have received this transmission in error, please notify us immediately by telephone to arrange for the return of the transmitted documents to us or to verify their destruction.

VERIFICATION OF TRANSMISSION OF PHI

Please contact _____ at _____ To verify receipt of this Fax or to report problems with the transmission.

I verify the receiver of this Fax has confirmed its transmission:

Name: _____ Date: _____ Time: _____
DHS Representative



Health Services
www.dhs.lacounty.gov



ATTACHMENT II

CONSENT TO PHOTOGRAPH AND AUTHORIZATION FOR USE OR DISCLOSURE

Patient Name: _____ MRUN: _____

Consent to Photograph; Authorization for Use and Disclosure

I hereby consent to be photographed while receiving treatment at the hospital. The term "photograph" includes video or still photography, in digital or any other format, and any other means of recording or reproducing images.

I hereby authorize the use of the photograph(s) by, or disclosure of the photograph(s) to:

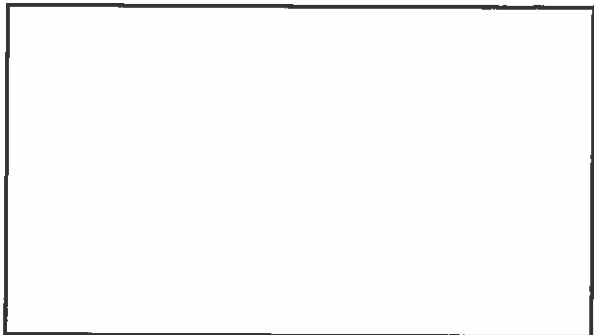
(Persons/Organizations authorized to receive the information)

(Address - street, city, state, zip code)

Purpose

I hereby authorize the use or disclosure of the photograph(s) for the following uses or purposes (describe permitted uses, e.g., dissemination to hospital staff, physicians, health professionals, and members of the public for educational, treatment, research, scientific, public relations, marketing, new media, and charitable purposes):

I consent to be photographed and authorize the use or disclosure of such photograph(s) in order to assist scientific, treatment, educational, public relations, marketing, news media, and charitable goals, and I hereby waive any right to compensation for such uses by reason of the foregoing authorization. I and my successors or assigns hereby hold the hospital, its employees, my physician(s), and any other person participating in my care and their successors and assigns harmless from and against any claim for injury or compensation resulting from the activities authorized by this agreement.



Consent to Photograph and Authorization for Use or Disclosure

Consent to Photograph and Authorization for Use or Disclosure

Expiration

This authorization expires (*insert date:*) _____

Upon expiration of this authorization, this hospital will not permit further release of any photograph, but will not be able to call back any photographs or information already released.

My Rights

I may request cessation of filming or recording at any time.

I may rescind this authorization up until a reasonable time before the photograph is used, but I must do so in writing and submit it to the following address:

I may inspect or obtain a copy of the photograph whose use or disclosure I am authorizing.

I may refuse to sign this authorization. My refusal will not affect my ability to obtain treatment or payment or eligibility for benefits.

I have a right to receive a copy of this authorization.

Information disclosed pursuant to this authorization could be re-disclosed by the recipient. Such re-disclosure is in some cases not protected by California law and may no longer be protected by federal confidentiality law (HIPAA).

I understand that I will not receive any financial compensation.

If this box is checked, the hospital will receive compensation for the use or disclosure of my photograph(s).

Signature

Date: _____ Time: _____ AM / PM

Signature: _____
(patient/representative/spouse/financially responsible party)

If signed by someone other than the patient, indicate relationship: _____

Print name: _____
(representative/spouse/financially responsible party)



ATTACHMENT III

CONSENTIMIENTO PARA LA TOMA DE FOTOGRAFÍAS Y AUTORIZACIÓN PARA SU USO O DIVULGACIÓN

Nombre del Paciente: _____ Número de Tarjeta: _____

Consentimiento para la Toma de Fotografías y Autorización para Su Uso o Divulgación

Por la presente, doy mi consentimiento para que se me tomen fotografías mientras recibo tratamiento en el hospital. El término "fotografía" incluye video o fotografía fija, en formato digital o de otro tipo, y cualquier otro medio de registro o reproducción de imágenes.

Por la presente, autorizo el uso o la divulgación de la(s) fotografía(s) por parte de:

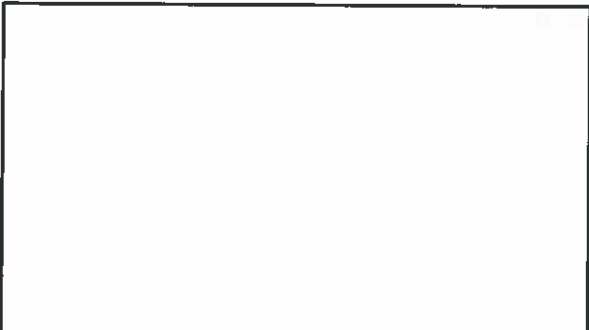
(Personas/Organizaciones autorizadas a recibir la información)

(Dirección: calle, ciudad, estado, código postal)

Propósito

Por la presente, autorizo el uso o la divulgación de la(s) fotografía(s) para los siguientes usos o propósitos (describa los usos permitidos, p. ej., difusión al personal del hospital, médicos, profesionales de la salud y miembros del público con fines educativos, de tratamiento, de investigación, científicos, de relaciones públicas, de mercadotecnia, de medios de comunicación y benéficos):

Doy mi consentimiento para que se me tomen fotografías y autorizo el uso o la divulgación de tal(es) fotografía(s) a fin de contribuir con los objetivos científicos, de tratamiento, educativos, de relaciones públicas, de mercadotecnia, de medios de comunicación y benéficos, y por el presente renuncio a cualquier derecho a recibir compensación por tales usos en virtud de la autorización precedente. Por la presente, yo y mis sucesores o cesionarios eximimos al hospital, a sus empleados, a mi(s) medico(s) y a cualquier otra persona que participe en mi atención, y a sus sucesores y cesionario, de toda responsabilidad ante cualquier reclamo por daños o de indemnización que surja de las actividades autorizadas por este acuerdo.



Consentimiento para la Toma de Fotografías y Autorización para Su Uso o Divulgación

Vencimiento

Esta autorización vence el (*insertar fecha:*) _____

Una vez que venza esta autorización, el hospital no permitirá posteriores divulgaciones de mi fotografía, pero no podrá pedir que se devuelvan las fotografías o la información ya divulgadas.

Mis Derechos

Puedo solicitar que cese la filmación o grabación en cualquier momento.

Puedo rescindir esta autorización hasta una fecha razonable antes de que se utilice la fotografía, pero debo hacerlo por escrito y enviar la rescisión a la siguiente dirección:

Puedo inspeccionar u obtener una copia de la fotografía cuyo uso o divulgación estoy autorizando.

Puedo negarme a firmar esta autorización. Mi negativa no afectara mi posibilidad de obtener tratamiento ni el pago o la elegibilidad para beneficios.

Tengo derecho a recibir una copia de esta autorización.

El destinatario podría volver a divulgar la información divulgada conforme a esta autorización. Tal nueva divulgación en algunos casos no está protegida por las leyes de California y podría ya no estar protegida por la ley de confidencialidad federal (HIPAA).

Entiendo que no recibiré ningún tipo de compensación financiera.

Si esta casilla está marcada, el hospital recibirá compensación por el uso o la divulgación de mi(s) fotografía(s).

Firma

Fecha: _____ Hora: _____ AM / PM

Firma: _____
(paciente/representante/cónyuge/parte económicamente responsable)

En caso de que lo firmase una persona que no sea el paciente, indique la relación:

Nombre en letra de imprenta: _____
(paciente/representante/cónyuge/parte económicamente responsable)