

# HIPAA (HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT)

## Primary Goals of the HIPAA Legislation

- Assure health insurance portability
- Reduce healthcare fraud and abuse
- Simplify electronic administrative processes
- Guarantee security and privacy of health information

HIPAA is the most sweeping legislation to affect healthcare since Medicare in 1965. Nearly everyone will be effected: payors, employers, providers, clearinghouses, practice management system vendors, billing agents, and service organizations. In regard to protecting patient information, security is defined as the protection of information, data and systems from accidental or intentional access by unauthorized users. Common threats to patient information security include talking about patients, using identifiable information such as names, diagnosis, etc, in public areas.

## Examples of Protected Health Information

- Clinical information
- Name and social security numbers
- Names of relatives, family name, and employer
- Health plan numbers and account numbers
- Telephone numbers, fax numbers and emails
- All dates related to the individual, ie, birth, etc
- Geographic subdivision smaller than state
- Any information that can reasonably identify a patient

## Penalties for Non-compliance with HIPAA Regulations

MONETARY PENALTY	TERM OF IMPRISONMENT	OFFENSE
\$100	N/A	Single violation of a provision.
Up to \$25000	N/A	Multiple violations of an identical requirement for prohibition made during a calendar year.
Up to \$50000	Up to 1 year	Wrongful disclosure of individually identifiable health information.
Up to \$100000	Up to 5 years	Wrongful disclosure of individually identifiable health information committed under false pretenses.
Up to \$250000	Up to 10 years	Wrongful disclosure of individually identifiable health information committed under false pretenses with intent to sell, transfer, or use for commercial advantage, personal gain, or malicious harm.

Failure to implement transaction sets can result in fines of \$225000 per year or more.  
**(\$25,000 per requirement, times nine transactions)**

Failure to implement privacy and security measures can result in imprisonment.

### Patients Rights

- Patients have the right to
  - Look at and obtain a copy of their health information.
  - Know how their health information has been used and to whom it has been disclosed.
  - File a formal complaint if their privacy has been violated.
  - Patient or parental consent must be obtained before a patient's health information can be released to family members.
  - Protecting patient information includes electronic, written and verbal communication.

### Notice of Privacy Practices

Covered Entities must provide a simple explanation of their privacy practices. Direct treatment providers must make a good faith effort to obtain written acknowledgment of receipt of the notice of privacy practices.

### Minimum Necessary

Employees should use only the information minimally necessary to do their job.

### Business Associates

Covered Entities may disclose PHI to business associates. They are required to have contracts that require their business associates to observe certain privacy standards listed in the regulations.

### **PERSONAL REPRESENTATIVES (PARENTS)**

- HIPAA gives control of a minor's PHI to the parent, guardian, or person acting in *loco parentis* with certain exceptions.
- HIPAA does not overturn state laws that give providers discretion to disclose PHI to parents or prohibit the disclosure of PHI to a parent.
- Verification of the personal representative's identity is a critical overlap with physical security.

### **PRIVACY DO'S**

- Immediately remove all patient health information from printers, fax machines and photocopiers.
- Dispose of protected health information in the appropriate confidential bin.
- When conducting a conversation regarding a patient, do so in a private place or speak quietly so you can't be overheard.
- Keep medical records and other documents containing personal health information out of public view.
- When possible, close patient/examining room doors or draw curtains and speak softly when discussing patient's health information.

- Treat other people's confidential information as if it were your own.
- Password protect your laptop computer and your personal digital assistant.
- Report privacy violations in the hospital to the Privacy Officer, at extension 12302 so we can improve our organization's privacy practices.

### **PRIVACY DON'TS**

- Don't share confidential patient information with anyone who doesn't need to know in order to do his or her job.
- Don't share passwords on your computer.
- Never access information about a patient unless you need it to do your job.
- Don't walk away from open medical records, lab results, or computers, etc. Close records first and use a bookmark, if necessary.



## Environment of Care for New Employees

Please keep this information and sign and return the enclosed statement indicating that you have read and understand your role in the safety, security, and environment of care at Children's Hospital Los Angeles.

### Emergency Codes (Ext. 33 except where noted)

- Code Blue - Medical Emergency
- Code Orange - Hazardous Material Spill
- Code Red – Fire Emergency
- Code Triage Internal or Code Triage External - Disaster Plan Activation (internal or external)
- Code Yellow – Bomb Threat (Ext. 711)
- Code Pink (infant) or Purple (toddler and above) Hospital Lockdown due to a Missing or Abducted Infant or Child (Ext. 711)
- Code Bert—Combative Person (4650 Sunset)
- Code Gray – Combative Person (off main campus)
- Code Silver – Person with Weapon and/or Active Shooter and/or Hostage Situation (Ext. 711)

### CHLA Identification Badges

- Your CHLA ID badge must be worn at all times when on the CHLA premises
- Your CHLA ID badge must be worn between the neck and waistline, with the photo facing forward
- If you lose or misplace your CHLA ID badge, you must report it immediately missing to Security (Ext. 12313) and the Parking Office (Ext. 12214)

### CHLA Visitor Passes and ID Badges

- All visitors to CHLA (whether parents, guardians, family members, vendors, etc.) must have a visible CHLA visitor pass or CHLA ID badge at all times while on the CHLA premises
- CHLA Visitor passes and badges are as follows:
- Green Badge – Parents, Legal Guardians or Caregivers to all inpatient care areas (1week pass)
- Yellow Pass – Visitors to inpatient units, OR/ASC (24hr pass)
- Orange Pass – Visitors to Outpatient/Clinic Areas
- Red Pass – Visitors to the Emergency Department
- Blue Badge – First Floor Lobby Pass
- Blue Pass – Other General Hospital Business
- White Pass or Badge – CHLA issued vendor pass or vendor ID badge

### Wrong Pass/Badge or No Pass/Badge

- All employees are responsible for:
- Escorting individuals without a CHLA issued visitor pass or ID Badge to the Guest Services Desk or the nearest Security Officer
- Asking if you can assist all individuals with the wrong visitor pass or ID badge who is in the wrong area. Example: Visitor with an orange pass is seen in an inpatient care area

### Safety

- Know your department's emergency procedures
- Know how to complete an *iReport* in the event something unusual happens to you or your patient
- Know how to report emergencies (Dial 33 or 711)
- Know how to access the CHLA Safety Management Plans and CHLA Policies and Procedures Libraries

Revised 09/03/2019

### Hazardous Materials/Waste

- Wear proper personal protective equipment
- Know how to properly dispose of chemicals
- Use appropriate labels on all chemicals that are used by you
- Know how to access the CHLA Safety Data Sheets for chemicals in your area

### Fire/Life Safety

- Safety of Life – Remove occupant and close the door
- Alarm – Activate a manual pull station and dial 33
- Fight the fire
- Evacuate – If there is danger or smoke

### Fire Extinguisher Use – PASS

- Pull the pin
- Aim
- Squeeze the handle
- Sweep the base of the fire

### Evacuation Procedures

- Evacuate horizontally beyond next fire/smoke door
- Evacuate vertically, two floors minimum or unit capable of receiving patient type
- Meet at designated assembly area
- Account for all evacuees
- Notify CHLA Incident Command Center at Ext. 16253 of status/missing persons of status/missing persons
- Evacuation Priority – those closest to danger, ambulatory, those you can move yourself, those you need help to move

### Emergency Preparedness/Disaster Procedures

- Code Triage Internal or Code Triage External will be communicated through the CHLA Emergency Mass Notification System, overhead page and your CHLA email
- All departments should fill out the unit status report (appendix D)
- All available hospital personnel report to the Command Center

### Medical Equipment Malfunction

- Biomedical Engineering is part of the IS department. All requests for medical equipment service should be submitted to the help desk at ext. 14444.
- Prior to use and regardless of ownership all medical equipment must be inspected by the Biomedical Engineering department.
- Sequester, along with its reusable supplies (ECG Cables etc.), any medical equipment suspected of causing harm and submit a service request through the help desk for pick up and investigation by Biomedical Engineering.

### Utilities Failure

- Know that the Hospital's emergency power generators will start in less than 10 seconds.
- Know that these power supply systems are tested on a weekly basis
- You may be needed to assist patients whose equipment has failed
- Know process to follow in event of utilization failure

<b>CHLA</b>	<b>HOSPITAL POLICY AND PROCEDURE MANUAL</b>			
	SUBJECT: Confidentiality of Information			
	ORIGINAL DATE: 03/01/1997	EFFECTIVE DATE: 05/09/18	PREVIOUS NAME/NUMBER:  ETH – 01.0	PAGE NUMBER:  Page 1 of 1
POLICY NUMBER: ADM – 107.0	CHAPTER: ADMINISTRATIVE		APPROVED BY: Chief Administrative Officer	

**PURPOSE:**

In order to protect the confidentiality of patient care and hospital matters, Children’s Hospital Los Angeles considers all information regarding its patients, their families, hospital employees and hospital business as confidential. All board members, officers, employees, volunteers, residents/fellows, and students, are required to adhere to this policy and not release or disclose any information without appropriate written authorization. The hospital complies with all applicable federal (HIPAA) and state law regarding the release and protection of health information.

**PROCEDURE:**

Board members, officers, employees, volunteers, residents/fellows, and students are asked to sign a statement of confidentiality when they begin their tenure with Children’s Hospital Los Angeles to acknowledge their awareness of and reaffirm their commitment to this policy.

This policy includes the confidentiality of medical staff records and procedures, all protected health information, employee personnel files, and information contained in the hospital computer systems, including the clinical information system (hereinafter referred to as KIDS and/or any other clinical system requiring a password) for Medical Staff and medical training staff. Regarding KIDS, each provider/clinician is required to use their assigned unique username also called sign-on access to the KIDS system. In addition, passwords and sign-ons must not be shared. KIDS passwords and sign-ons will be assigned only when all paperwork has been submitted, clearance has been given, a provider number assigned, and training on the KIDS systems has been successfully completed.

Board members, officers, employees, volunteers, residents/fellows, and students are also asked to refrain from discussing any patient information or hospital business in any inappropriate area, including corridors, elevators, the HBO Cafe, hospital lobbies, or waiting rooms.

All areas within the hospital campus shall ensure that patient identifying information and diagnosis are not available to the public through any device, mechanism or process.

**POLICY OWNER:**

*Chief Compliance Officer*

<b>CHLA</b>	<b>HOSPITAL POLICY AND PROCEDURE MANUAL</b>			
	SUBJECT: Social Media			
	ORIGINAL DATE: 04/15/2009	REVISED DATE: 03/23/2021	PREVIOUS NAME/NUMBER:  MHR-14.0; HR – 63.0	PAGE NUMBER:  Page 1 of 8
POLICY NUMBER: ADM – 269.0	CHAPTER: ADMINISTRATIVE		APPROVED BY: Quality Improvement Committee, Chief Clinical Officer, Medical Executive Committee, Board of Directors	

## PURPOSE

This policy applies to CHLA workforce members using social media in a manner that discloses their affiliation or employment with CHLA, represents their views as being those of the institution or from which users of the platform could reasonably presume that their views are those of the institution. These guidelines represent best practice and are designed to protect CHLA, its team members, affiliated physicians or practitioners, patients and their families from any harm that might result through the misuse of social media.

This Policy also clarifies the organization’s purview and that it may access or review workforce members’ publicly accessible social media posts, messages and account information at any time; the contents therein may be subject to scrutiny by hospital representatives to ensure consistency with its mission and alignment with the hospital’s policies and associated legal and compliance requirements.

## TERMS AND DEFINITIONS

Children’s Hospital Los Angeles (henceforth referred to as “CHLA” or “the hospital”) is committed to conducting business in compliance with all applicable laws, regulations and CHLA policies and in a manner consistent with our organization’s mission, values and guiding behaviors.

An exhaustive list of online communication and social computing channels, media, networking, and platforms cannot be compiled, but is broadly defined as being websites or platforms where content is generated or submitted by users. Examples include, but are not limited to, blogs, forums, video sharing and social networking sites including but not limited to Facebook, Health Grades, Instagram, LinkedIn, Pinterest, Twitter, Yelp, Snapchat, Reddit, TikTok, Twitch, Discord, Parler, blog comments, Next Door, and YouTube.

## SCOPE

This Policy applies to all CHLA employees, agents, clinicians, contractors, volunteers, vendors or other individuals or entities retained to fulfill the organization’s mission. For simplicity, this group shall be referred to throughout as “employees,” “user” or “users.”

## POLICY

The institution prohibits workforce members from engaging in social media and online interactions when those activities threaten the security, integrity and privacy of CHLA’s

---

<b>CHLA</b>	<b>HOSPITAL POLICY AND PROCEDURE MANUAL</b>			
	SUBJECT: Social Media			
	ORIGINAL DATE: 04/15/2009	REVISED DATE: 03/23/2021	PREVIOUS NAME/NUMBER:  MHR-14.0; HR – 63.0	PAGE NUMBER:  Page 2 of 8
POLICY NUMBER: ADM – 269.0	CHAPTER: ADMINISTRATIVE		APPROVED BY: Quality Improvement Committee, Chief Clinical Officer, Medical Executive Committee, Board of Directors	

confidential information. All social media references or imputations that relate to CHLA should occur at the direction or under the auspices of the Marketing and Communications Department.

### COMPLIANCE WITH HOSPITAL POLICIES

Workforce members must not violate any of the hospital’s policies, procedures or guidelines online or offline.

### SOCIAL COMPUTING GUIDELINES FOR WORKFORCE MEMBERS

Workforce members will be held personally, professionally, and legally responsible for any content that they publish online without proper authorization. When an online interaction impacts or implicates CHLA, the guidelines below must be followed.

1. **Social Media Channels** - Workforce members should not create social media identities, channels and/or accounts that could be interpreted to represent the hospital or a division, program or professional reputation without authorization by the Chief Marketing Officer and ongoing oversight and guidance from the Marketing Communications Department. Creation and management of any social media account or identity that could have an impact on the hospital’s brand or reputation in any way is the responsibility of the Marketing Communications Department. You can reach out to social@chla.usc.edu for questions.
2. **Authorized speakers** – Only individuals with fiscal responsibility for the enterprise and all others as deputized by the Public Relations team are authorized to speak on behalf of the organization. If you are authorized to speak on behalf of CHLA you must state your position and the limits of your authority.
3. **Protecting Patient Privacy** - Workforce members may not post or publish patient information, including a patient’s health information, unless at the direction of the Marketing Communications department. This includes, but is not limited to, posting updates about a patient or a patient’s condition on the workforce members own social media account or other social media channels (with or without personal identifiers), posting or tagging photos or videos of patients and family members, writing reviews or commenting on other people’s reviews, live streaming, Snapchatting, blogging, microblogging, tweeting, liking or sharing information about patients and their family members.
4. **Use of Institutional Email Address** - Workforce members should refrain from using their institutional email address as the login for a personal social media presence. This is designed to ensure that, should an individual leave the organization and an account or password needs to be recovered or reset, the workforce member is at complete liberty to retain long-term interest in their own social media accounts. It also goes further to establish a stronger boundary between the thoughts and opinions of an individual and the official stance of the

<h1>CHLA</h1>	<b>HOSPITAL POLICY AND PROCEDURE MANUAL</b>			
	SUBJECT: Social Media			
	ORIGINAL DATE: 04/15/2009	REVISED DATE: 03/23/2021	PREVIOUS NAME/NUMBER:  MHR-14.0; HR – 63.0	PAGE NUMBER:  Page 3 of 8
POLICY NUMBER: ADM – 269.0	CHAPTER: ADMINISTRATIVE		APPROVED BY: Quality Improvement Committee, Chief Clinical Officer, Medical Executive Committee, Board of Directors	

institution on any health care or health-related topic. Exceptions to this policy will be made in cases where the user must use their institutional email address for the professional management of an institutionally owned and operated social media presence (for which authorization by CHLA’s Marketing and Communications Department leadership is required as indicated above).

5. **Social Media Interactions with Patients and Families** - Workforce members must recognize that their relationships with CHLA patients (and their family members) are **professional relationships** and that social pleasantries shared at the bedside do not extend into online social networking. Because social networking blurs the lines of patient-clinician relationships, workforce members are strongly discouraged from “friending”, “liking” or “sharing” patients’ and their family members or accepting friend requests from patients and their family members. Moreover, any romantic, sexual, or intimate physical or verbal relationships or discussions between workforce members and patients and their family members are prohibited via social media, much as they would be in the workplace. This is designed to ensure that workforce members are able to maintain their professional objectivity and maximize their ability to care for patients, and maintain the trust that they wish to enjoy with every patient and their family that they treat in the future.
  - a. Exception  
An exception to the policy regarding social media interactions with patients and families is permitted in instances when a workforce member has a pre-existing relationship with a family prior to their child becoming a CHLA patient. In such instances, workforce members must be extremely careful to prevent their online engagement from straying into discussion of anything related to the patient’s medical care or health status).
  
6. **Online Conduct** - Workforce members should be mindful that all of their engagement online should be reflective of CHLA’s high standards of professional conduct, especially if they link or tie themselves to CHLA in any way. Managers and executives, by virtue of their positions, must assume that workforce members and direct reports will read their social media content and bear in mind that their personal thoughts may be construed as representative of hospital policy, opinion, and strategy and that public forums are not the place to communicate hospital policies to employees. Workforce members should remember that misconduct that they self-report or document online is often reported by the community to CHLA’s HR, Marketing, and Compliance teams.
  
7. **Harassment** - Team members are prohibited from using social networking to unlawfully harass, abuse, discriminate against, threaten violence against, or make malicious, obscene or defamatory statements about CHLA’s employees, affiliated physicians, other healthcare providers, volunteers, students, patients, guests, vendors or contractors. In other words (and consistent with CHLA’s



<h1>CHLA</h1>	<b>HOSPITAL POLICY AND PROCEDURE MANUAL</b>			
	SUBJECT: Social Media			
	ORIGINAL DATE: 04/15/2009	REVISED DATE: 03/23/2021	PREVIOUS NAME/NUMBER:  MHR-14.0; HR – 63.0	PAGE NUMBER:  Page 4 of 8
POLICY NUMBER: ADM – 269.0	CHAPTER: ADMINISTRATIVE		APPROVED BY: Quality Improvement Committee, Chief Clinical Officer, Medical Executive Committee, Board of Directors	

values): Be respectful. Harassment includes but is not limited to offensive social media posts or other offensive content which could contribute to a hostile work environment on the basis of race (including traits historically associated with race), sex/gender (including pregnancy), disability, religion, creed, color, gender identity or expression, transgender status, reproductive health decision making, national origin, sexual orientation, predisposing genetic characteristics or carrier status, age, ancestry, military status, arrest/conviction record, familial status, protected veteran status or any other status protected by local, state or federal law. This requirement is not intended to limit, or infringe on Section 7 or Section 8(a)(1) rights under the National Labor Relations Act.

8. **Medical Questions** - Should workforce members be approached with a medical question via social media, they are allowed to respond as follows: *“Unfortunately, we are unable to provide medical advice through this medium. If this is an emergency, we suggest going to the nearest available emergency room. If you would like to see a specific department, please call 323-660-2450.”*

## RESPONDING TO SOCIAL MEDIA COMMENTS OR RATINGS FROM PATIENTS AND FAMILIES

### Social Media Platforms

Even if a patient or family member indicates that they receive medical care from specific CHLA team members, those team members are not thereby granted permission to respond in kind or at all to those posts. Responding may violate the patient’s privacy rights as well as possible HIPAA violation(s) and may result in disciplinary action.

### Rating Websites

As it pertains to ratings of providers or their care, CHLA Workforce members must not respond to any online comment left by a patient or family member of a patient online. Such action may violate the patient’s privacy rights as well as possible HIPAA violation(s) and may result in disciplinary action. Instead, CHLA workforce members should:

1. Alert the Patient Relations department at 323-361-4682 or 323-361-4198.
2. Alert the Marketing Communications department at 323-361-7691.

## MAINTAIN CONFIDENTIALITY ABOUT HOSPITAL NEWS OR BUSINESS

Workforce members may not disclose CHLA confidential information. See ADM 107 Confidentiality of Information. Workforce members are not permitted to share news about any official hospital business online until it has been officially shared by the hospital through a news story, press release or placement on the hospital’s website or social media channels, such as strategic plans or operational developments, and visits from celebrities or political figures.

<b>CHLA</b>	<b>HOSPITAL POLICY AND PROCEDURE MANUAL</b>			
	SUBJECT: Social Media			
	ORIGINAL DATE: 04/15/2009	REVISED DATE: 03/23/2021	PREVIOUS NAME/NUMBER:  MHR-14.0; HR – 63.0	PAGE NUMBER:  Page 5 of 8
POLICY NUMBER: ADM – 269.0	CHAPTER: ADMINISTRATIVE		APPROVED BY: Quality Improvement Committee, Chief Clinical Officer, Medical Executive Committee, Board of Directors	

## **CELEBRITY OR VIP VISITS**

In cases where celebrities visit the hospital to cheer up patients and their family members, these visits should be considered official hospital business and no information should be shared about those visits other than what is officially posted by the organization.

Workforce members must NEVER approach or take a photo of a celebrity or VIP without express permission being granted by a Foundation or Marketing workforce member ahead of the visit. Workforce members should consult with the CHLA workforce members coordinating the celebrity's visit to determine whether personal photos may be taken and must delay posting photos or other details about the visit to social media until released to do so. Workforce members should be aware that these celebrities and VIPs may be visiting the hospital for personal or private reasons and it is paramount that these visits be handled with the utmost sensitivity and patient care should take priority. For questions regarding the timing of the release of personal photos, please check with your supervisor or the Celebrity and VIP office at 323-361-4121. In all cases, workforce members are advised to work with their managers and hospital leadership before sharing CHLA news so that proper steps can be taken to release news through the most appropriate channels.

## **LEGAL COMPLIANCE**

Workforce members must comply with all copyright, fair use and financial disclosure laws when posting online.

## **ADVERTISING**

Advertising (including print and digital) for any part of the hospital is the role of the Marketing Communications Department. Employees should not engage in these activities or work with independent agencies without the direct oversight of the Marketing Communications Department.

## **IMPACT ON WORKFORCE MEMBERS' RESPONSIBILITIES**

Social media engagement must not alter workforce members' ability to perform their job duties or responsibilities. Workforce members should refrain from using social media while on work time, unless it is work-related, authorized by the user's manager, and consistent with the parameters of this Policy. Personal social media use should be confined to break periods and personal computing equipment, and should not be accessed on CHLA-owned property and systems.

## **MONITORING AND TRACKING**

The hospital may monitor the usage of its computing assets at any time (for additional information,

---

<h1>CHLA</h1>	<b>HOSPITAL POLICY AND PROCEDURE MANUAL</b>			
	SUBJECT: Social Media			
	ORIGINAL DATE: 04/15/2009	REVISED DATE: 03/23/2021	PREVIOUS NAME/NUMBER:  MHR-14.0; HR – 63.0	PAGE NUMBER:  Page 6 of 8
POLICY NUMBER: ADM – 269.0	CHAPTER: ADMINISTRATIVE		APPROVED BY: Quality Improvement Committee, Chief Clinical Officer, Medical Executive Committee, Board of Directors	

refer to CHLA Policy [HR – 35.0 Privacy Searches and Investigations](#) and [MIS - 33.0 Workspace Acceptable Use and Security](#)). Social media posts are often readily accessible to the public and, as a result, hospital representatives may be able to view workforce members’ online interactions, even if they have been made from personal devices or on their own time. The hospital's brand, likeness, and patient privacy data (including but not limited to HIPAA, intellectual property, financial data, personal information, and other confidential data) are monitored for unauthorized use by third-party tools.

#### Monitoring and Tracking for Workforce Member’s Productivity

Though neither the Information Services Department nor the Marketing and Communications Department makes any commitment to monitor social computing activities of workforce members, if managers or supervisors believe that social media use is interfering with completion of job duties or functions, they may elect to monitor workforce members on an individual basis on CHLA property and incorporate this information into performance reviews. These requests can be made through the I.S. Service Desk at ext. 14444.

#### Monitoring and Tracking for Use of Brand Name or Mark

As part of CHLA’s monitoring of the use of its brand, CHLA may come across statements made on social media channels that would not otherwise be public, or channels created that leverage the CHLA brand inappropriately.

### **PERSONAL OPINION STATEMENT**

If you have personal social media channels and comment online in a manner that bridges on CHLA’s brand or on topics related to child health or pediatric medicine, we encourage you to use the following statement to separate your personal role vs. professional role.

1. Make it clear that your opinions are not those of your employer or affiliated hospital. The easiest way to accomplish this is by inserting the verbiage below (taken from our Social Computing Policy):

*“The postings I make on this site are my own personal opinions and do not reflect the opinions or views of Children’s Hospital Los Angeles.”*

2. Include this language on your social media profile page (bio).
3. Deliver the information in a professional voice and tone.
4. Remember posts, conversations and exchanges may remain in public or be searchable over a long period of time (even long after you may have deleted the original post).
5. Many social networking sites are not secure and may be available to anyone with access to a computer and internet. Posts may be photographed or copied and shared without the background

<h1>CHLA</h1>	<b>HOSPITAL POLICY AND PROCEDURE MANUAL</b>			
	SUBJECT: Social Media			
	ORIGINAL DATE: 04/15/2009	REVISED DATE: 03/23/2021	PREVIOUS NAME/NUMBER:  MHR-14.0; HR – 63.0	PAGE NUMBER:  Page 7 of 8
POLICY NUMBER: ADM – 269.0	CHAPTER: ADMINISTRATIVE		APPROVED BY: Quality Improvement Committee, Chief Clinical Officer, Medical Executive Committee, Board of Directors	

of a prior conversation or context in which the views were shared.

6. It is the responsibility of the team member/provider to conduct themselves online in such a way that furthers our mission of providing a quality healthcare environment for all.

## RATING WEBSITES

If a workforce member rates, reviews or gives an online opinion (e.g., Yelp, Glassdoor, Google Reviews, Indeed, Facebook Reviews) about the hospital, employees, its policies, programs, units, departments or divisions, the user should indicate their role, and incorporate the following statement:

*“The postings I make on this site are my own personal opinions and do not necessarily reflect the opinions or views of Children’s Hospital Los Angeles.”*

Workforce members should not imply official endorsement, approval or sanction for an individual, organization, program, association, vendor or entity online on behalf of the hospital in compliance with hospital policy, see the full policy by downloading this PDF: [ADM - 30.0 Hospital Name Use to Imply Sponsorship of Product or Individual Views](#).

## SOCIAL MEDIA INTERACTION WITH OTHER WORKFORCE MEMBERS

Workforce members must recognize that their relationships with fellow colleagues are **professional relationships**. Social media interactions between workforce members (for example, accepting or rejecting “friend” requests) must align with all of the hospital’s policies, procedures, and guidelines and not result in or be used for harassment, bullying, intimidation, unlawful, or other discriminatory behaviors). Nothing in this policy is intended to infringe upon workforce members’ rights to engage in concerted activities under Section 7 of the National Labor Relations Act.

## REPORTING

If you see any online misconduct or violation of this Social Media Policy by any workforce members, you may share your observations with Human Resources. Misconduct or violations of this social media policy may be monitored by third-party tools (see Monitoring and Tracking section above).

## NON-COMPLIANCE (Violations of Policy)

Any failure to abide by this Policy may result in disciplinary action involving revoking or restricting any right to system access and may lead to more serious disciplinary action in accordance with CHLA disciplinary policies up to and including termination of employment and legal liability for hospital workforce members. For non-CHLA workforce or non-employed, credentialed and privileged practitioners, violations will be forwarded to the Medical Staff Services Department for management through the Medical Staff process.

<b>CHLA</b>	<b>HOSPITAL POLICY AND PROCEDURE MANUAL</b>			
	SUBJECT: Social Media			
	ORIGINAL DATE: 04/15/2009	REVISED DATE: 03/23/2021	PREVIOUS NAME/NUMBER:  MHR-14.0; HR – 63.0	PAGE NUMBER:  Page <b>8</b> of <b>8</b>
POLICY NUMBER: ADM – 269.0	CHAPTER: ADMINISTRATIVE		APPROVED BY: Quality Improvement Committee, Chief Clinical Officer, Medical Executive Committee, Board of Directors	

## RESOURCES

### [CHLA Social Media Intranet Page](#)

This resource provides access to a social media guide for workforce members, a link to this policy, social media FAQs, Do's and Don'ts for workforce members and presentations which can be used in workforce member meetings to clarify institutional expectations.

## REFERENCES

1. CHLA Policy: [ADM - 30.0 Hospital Name Use to Imply Sponsorship of Product or Individual Views](#)
2. CHLA Policy: [HR – 35.0 Privacy Searches and Investigations](#)
3. CHLA Policy: [MIS - 33.0 Workspace Acceptable Use and Security](#)

## POLICY OWNER

*Director, Digital Marketing*