UCLA Policy 410: Access without Consent to Electronic Communications Records

Issuing Officer: Chief Compliance and Audit Officer

Responsible Department: Compliance

Effective Date: DRAFT — 3/3/2021

Status: Supersedes August 16, 2010

ATTACHMENT A. PURPOSE & SCOPE

This Policy implements the provisions of the University of California Electronic Communications Policy (ECP) relevant to nonconsensual access (hereafter referred to as "access without consent") to University Electronic Communications Records. This Policy, consistent with the ECP, also addresses Electronic Communications Records for preservation of evidence and investigations.

This Policy applies to all Holders of Electronic Communications Records about or relating to University activities.

ATTACHMENT B. DEFINITIONS

For the purposes of this Policy:

See Definitions

ATTACHMENT C. POLICY STATEMENT

The University must obtain a Holder's consent prior to any access to Electronic Communications Records in the Holder's Possession for the purposes of examination or disclosure of University Electronic Communications Records, except under circumstances as outlined in and in accord with Section Access without Consent of this Policy.

University employees must comply with University requests for access to Electronic Communications Records in their Possession that pertain to the activities of the University, or whose disclosure is required to comply with applicable laws.

Except for UCLA Emeritus faculty and UCLA Emeritus staff, and Registered Students, or unless pursuant to an agreement for continuing provision of an Electronic Communications Service (including eligibility for Bruin OnLine services), employees who have separated from the University of California are no longer the Holders of Electronic Communications Records. The University can access these Records without consent and without following the provisions of Section Access without Consent from the point of separation. Nevertheless, when access to such Records is needed, least perusal of contents and the least action necessary to resolve the situation must still be employed.

Providers of University Electronic Communications Systems and Services must ensure that their operational practices and terms of service are consistent with this Policy, and that their users are made aware of these terms prior to use.

Unit heads must ensure that their local practices regarding Electronic Communications Records are consistent with this Policy, and that users are made aware of these practices as part of the onboarding process. Guidance can be found in the Electronic Communications Policy, Attachment 2 (Implementation Guidelines), Section III.B.5 on Access to University Administrative Records.

ATTACHMENT D. ACCESS WITHOUT CONSENT

The University can access Electronic Communications Records without the consent of the Holder for the purposes of examination or disclosure of the contents only when:

(i) required by and consistent with law;

(ii) there is Substantiated Reason to believe that violations of law or of University policies listed in the ECP Appendix C, Policies Relating to Access Without Consent have taken place;

(iii) there are Compelling Circumstances; or

(iv) under Time-dependent, Critical Operational Circumstances.

Part I. Authorization

When under the circumstances described above and in accordance with the appropriate procedure outlined below, the contents of Electronic Communications Records can be accessed, examined or disclosed without the Holder's consent.

Prior Authorization (Section Prior Authorization)

Emergency Circumstances (Section Emergency Circumstances)

Search Warrants and Subpoenas (Section Search Warrants and Subpoenas)

Preservation of Evidence (Section Preservation of Evidence)

California State and Internal Audit (Reference References.On March 18, 2004 the Regents Committee on Audit approved changes to the Internal Audit Management Charter authorizing Internal Audit to have access to University information except where prohibited by law. [http://www.universityofcalifornia.edu/regents/regmeet/mar04.html])

Prior Authorization

UCLA employees or investigative offices may request access without consent by completing Request Form for Authorization to Access Electronic Communications Records without Consent, Request Form for Authorization to Access Electronic Communications Records ("Request Form") in advance of access. The UCLA Authorizing Official is the official responsible for authorizing or denying the access request, in writing. Any authorization will be limited to the least perusal of contents and the least action necessary to resolve the situation.

The appropriate UCLA Authorizing Official depends upon the status of the affected Holder (see Table 1 below). Prior to approving or not approving the request, the UCLA Authorizing Official will seek the advice of the following officials and all such advice will be given in a timely manner.

- Department Head or Unit Head, to ensure the request is appropriate and related to University activities;
- Campus Counsel (if a campus matter) or UCLA Health Legal Affairs (if a Health Sciences matter) because of changing interpretations by the courts of laws affecting the privacy of Electronic Communications, and because of potential conflicts among different applicable laws;
- Chair of the UCLA Academic Senate, when a request involves Electronic Communications Records held by Faculty or Emeritus Faculty, will attach written advice separately from the Request Form; and
- Campus Chief Privacy Officer (if a campus matter) or UCLA Health Chief Privacy Officer (if a Health Sciences matter), on limiting authorization to the least perusal and the least action necessary to resolve the situation.

Table 1. UCLA Authorizing Officials

If Holder's Status is:	The UCLA Authorizing Official is:	The UCLA Authorizing Official is advised by:
Faculty, Emeritus Faculty	Vice Chancellor, Academic Personnel	• Department or Unit Head • Campus Counsel or UCLA Health Legal Affairs • Campus or UCLA Health Chief Privacy Officer • Chair, Academic Senate
Student (Not in a capacity as a Staff Employee)	Vice Chancellor, Student Affairs	• Campus Counsel or UCLA Health Legal Affairs • Campus or UCLA Health Chief Privacy Officer
Staff Employee (Non-UCLA Health), Student in this capacity, or Emeritus Staff	Administrative Vice Chancellor	• Department or Unit Head • Campus Counsel • Campus Chief Privacy Officer
UCLA Health Staff Employee or Student in this capacity	President of UCLA Health; CEO of UCLA Hospital System; and Associate Vice Chancellor of UCLA Health Sciences Vice Chancellor, UCLA Health Sciences; and CEO of UCLA Health	• Department or Unit Head • UCLA Health Legal Affairs • UCLA Health Chief Privacy Officer
Any	Chancellor	• Campus Counsel or UCLA Health Legal Affairs
Any	Executive Vice Chancellor and Provost	• Campus Counsel or UCLA Health Legal Affairs

The Chancellor or the Executive Vice Chancellor and Provost may act in place of any of the UCLA Authorizing Officials in Table 1, regardless of the affected Holder's status. A UCLA Authorizing Official will recuse themselves in the event of a conflict of interest. The authority of UCLA Authorizing Officials may not be delegated.

Authorization is given to the individual UCLA employee named in Request Form for Authorization to Access Electronic Communications Records, unless this request is from an investigative office (Section Investigations), in which case authorization is for that office.

Emergency Circumstances

In Emergency Circumstances, access without consent may be taken immediately without prior authorization, but appropriate authorization must then be sought without delay following the procedures described above. The least perusal of contents and the least action necessary is required to resolve the emergency.

If the action taken is not subsequently authorized, the Electronic Communications Holder may seek recourse (Section UCLA Recourse).

Search Warrants and Subpoenas

Search warrants and subpoenas are not subject to Sections Authorization.Prior Authorization, Emergency Circumstances, Investigations, Compliance with Law or UCLA Recourse. Search warrants and subpoenas for Electronic Communications Records will be referred to Campus Counsel or designated campus officials.

> *Search Warrants.* Duly signed search warrants will be processed in accordance with federal and state laws, University policies, and instructions in the warrant.

Subpoenas. Subpoenas will be processed in accordance with applicable federal and state laws and University policies (see UCLA Procedure 120.1, Producing Records Under Subpoena Duces Tecum and Deposition Subpoenas).

Campus officials will provide advance notice to individuals whose records are the subject of a subpoena or warrant, except where a court order prohibits such notice.

Investigations

The following investigative offices may act as the requestor for access without consent in Request Form for Authorization to Access Electronic Communications Records without Consent:

ADA/504 Compliance

Civil Rights Office

1. Discrimination Prevention
2. Title IX
3. Staff, Diversity & AA/EEO Compliance

Compliance

4. UCLA Compliance
5. UCLA Health Compliance Services

Human Resources

6. Campus Human Resources
7. Human Resources (UCLA Health)

Locally Designated Official

Research Policy and Compliance

Student Conduct

Part II. Notification

The campus or UCLA Health Chief Privacy Officer, as appropriate, will at the earliest opportunity that is lawful and consistent with other University policies notify the affected individual of the action(s) taken and the reasons for the action(s) taken. Campus Counsel or UCLA Health Legal Affairs, as appropriate, will advise if notification should not occur.

Each campus will issue, in a manner consistent with law, an annual report summarizing instances of authorized or Emergency Circumstances access without consent pursuant to the provisions of this section, without revealing personally identifiable data. The campus Chief Privacy Officer shall tabulate this data for the campus and provide the report as required by the ECP.

Part III. Compliance with Law

Actions taken under this Policy, including access to Electronic Communications Records residing on computers not owned or housed by the University, shall be in full compliance with the law and other applicable University policies, including laws and policies listed in ECP Appendix B, References. Advice of counsel must always be sought prior to any action involving Electronic Communications Records.

Should any requirement of this Policy be in conflict with legal requirements, Campus Counsel or UCLA Health Legal Affairs, as appropriate, in consultation with other campus offices or officials as appropriate, shall make a recommendation to the Executive Vice Chancellor and Provost or to the Chancellor about resolving the conflict.

Part IV. UCLA Recourse

A UCLA Electronic Communications Holder who believes that an action taken under Section Prior Authorization or Emergency Circumstances by employees or agents of the University was in violation of this Policy may file a complaint with [].

ATTACHMENT E. PRESERVATION OF EVIDENCE

Consent is not required to carry out the University's duty to preserve evidence. However, evidence subject to this Policy remains subject to this Policy when preserved. Thus any examination or disclosure of such preserved evidence requires the Holder's prior consent as required by Section Policy Statement, Policy Statement, or the procedure in Section Access without Consent, Access without Consent.

Preservation applies to all University Electronic Communications Services, including but not limited to departmental services, Enterprise Messaging, MedNet, Bruin OnLine, and Google Apps for UCLA.

Actual preservation shall be coordinated through the campus e-discovery Coordinator, or UCLA Health e-discovery Coordinator, as appropriate, to ensure preservation meets chain of custody and other legal requirements, and to ensure that preserved evidence is securely stored. Evidence so preserved may be exempted from the encryption requirements of UCLA Policy 404, Encryption of Electronically Stored Personal Information.

Preserved evidence will be released by the campus e-discovery Coordinator or UCLA Health e-discovery Coordinator in accordance with preserved evidence disposition protocols.

ATTACHMENT F. REFERENCES

Attachment G. University of California Electronic Communications Policy (ECP)

Attachment H. UCLA Procedure 120.1, Producing Records Under Subpoena Duces Tecum and Deposition Subpoenas

Attachment I. UC Whistleblower Policy

Attachment J. On March 18, 2004 the Regents Committee on Audit approved changes to the Internal Audit Management Charter authorizing Internal Audit to have access to University information except where prohibited by law. [http://www.universityofcalifornia.edu/regents/regmeet/mar04.html]

ATTACHMENT K. ATTACHMENTS

Attachment L. Request Form for Authorization to Access Electronic Communications Records.

Attachment M. Definitions

Issuing Officer

/s/

Chief Compliance and Audit Officer

Questions concerning this Policy should be referred to the

Responsible Department listed at the top of this document

Attachment N. Request Form for Authorization to Access Electronic Communications Records without Consent

HOW TO USE THIS FORM

For information about the use of this form, see UCLA Policy 410: Access without Consent to Electronic Communications Records.

Instructions to the UCLA Employee or Investigative Unit ("Requestor") to request authorization

RESPONSIBLE INDIVIDUAL	ACTION	NOTES
Requestor	a.i.1. Fill out Parts Request Details and Explanation of Need (Confidential) of this form.	Guidance may be obtained from Campus Counsel, UCLA Health Legal Affairs, or the campus or UCLA Health Chief Privacy Officers.
	a.i.2. Obtain the signature of the Electronic Communications Holder's department / unit head on Signatures of the form.	
	a.i.3. Take this form to Campus Counsel (for campus matters) or Health Legal Affairs (for Health Sciences matters), for their signature.	
Campus Counsel or UCLA Health Legal Affairs	a.i.4. Campus Counsel or Health Legal Affairs will obtain the remaining signatures.	
Campus or UCLA Health Chief Privacy Officer	a.i.5. The Chief Privacy Officer will remove Explanation of Need (Confidential) of this form and send a copy of Request and Signatures to the Requestor.	The original completed form will be retained by the appropriate Chief Privacy Officer.

If access is authorized by the UCLA Authorizing Official

RESPONSIBLE INDIVIDUAL	ACTION	NOTES
Requestor or representative of the investigative office (UCLA Policy 410, Section Investigations)	a.i.6. Present Parts Request and Signatures to the appropriate technical administrator who can provide access to the records requested. Parts Request and Signatures of this form may also be presented to specific individuals who must access or analyze the content. *[Note: These two Parts of the form are expected to exist on a single page in printed form.]*	Any access authorized is limited to the least perusal of contents and the least action necessary to resolve the matter. Any accessed content must be safeguarded as per UC IS3 Electronic Information Security. Individuals who access this content are not permitted to disclose or otherwise use what they have observed if not germane to the authorized purpose. However, if improper governmental activity (including violations of law or University policy) is inadvertently discovered or suspected during access, reporting of such violations shall be consistent with the UC Whistleblower Policy.
Requestor	a.i.7. The requestor will work with the campus or UCLA Health Chief Privacy Officer, as appropriate, to provide notification to affected individual(s) as required by UCLA Policy 410,	

Section Notification.

PART I. REQUEST DETAILS

INFORMATION ABOUT THE REQUEST

Who is making this request?

Name _____

Title _____

Department/Unit _____

Date of Request _____

Is this request for an investigation? (Restricted to departments listed in Policy 410, Investigations.)
■ Yes ■ No

If Yes, request is on behalf of, and authorization is for, the Department listed, not the individual.

What is the basis for this request?

ECP provisions under which Records are being sought (check all that apply)

- ☐ Required by and consistent with law
- ☐ Reasonable belief of violation of law or UC Policy
- ☐ Compelling Circumstances
- ☐ Time-dependent, critical operational circumstances

Reason(s) why Holder's consent cannot be obtained (check all that apply)

- ☐ Holder has denied a request to allow access
- ☐ Absence, illness, or death precludes requesting Holder's consent
- ☐ Compelling Circumstances preclude requesting the Holder's consent

Timing of request (check one)

- ☐ Request prior to access as required by the UC Electronic Communications Policy
- ☐ Request after access under Emergency Circumstances (see UCLA Policy 410, Section Emergency Circumstances)

Are the Records being sought from evidence previously preserved under UCLA Policy 410, Section Preservation of Evidence?

- ☐ Yes
- ☐ No

RECORDS SOUGHT

Who is the Holder of the Electronic Communications Record(s) being sought?

Name _____

Department/Unit _____

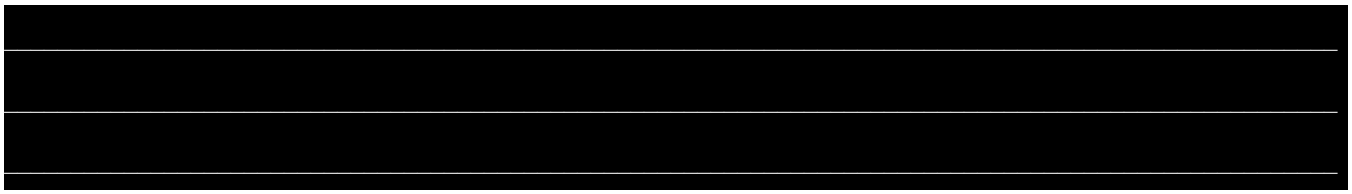
Detailed description of what Electronic Communications Records are being sought

(Attach a separate sheet if necessary.)

_____

_____

_____



Attachment B: Definitions

PART I. SIGNATURES

REQUIRED SIGNATURES (SEE UCLA POLICY 410, TABLE 1)

Does:	Recommend access without consent?	Sign and date
1. Department / unit head of Electronic Communications Holder	☐ Yes ☐ No ☐ N/A	Signature _____ Date _____
2. Counsel ☐ Campus Counsel ☐ UCLA Health Legal Affairs	☐ Yes ☐ No	Signature _____ Date _____
3. Chief Privacy Officer ☐ Campus ☐ UCLA Health	☐ Yes ☐ No ☐ N/A	Signature _____ Date _____
4. Chair, Academic Senate (only if the Holder is a Faculty or Emeritus Faculty member; attach written advice separately)	☐ Yes ☐ No ☐ N/A	Signature _____ Date _____

AUTHORIZING OFFCIAL'S SIGNATURE (SEE UCLA POLICY 410, TABLE 1)

Is access without consent authorized?

☐ Yes — Authorization is limited to the least perusal of contents and the least action necessary to resolve the situation.
☐ No

_____ _____
Signature of UCLA Authorizing Official — check corresponding box below Date

☐ Administrative Vice Chancellor
☐ Vice Chancellor, Academic Personnel
☐ Vice Chancellor, Student Affairs
☐ Vice Chancellor, UCLA Health Sciences; and CEO, UCLA Health
☐ Associate Vice Chancellor, UCLA Health Sciences; President, UCLA Health; and CEO, UCLA Hospital System
☐ Chancellor
☐ Executive Vice Chancellor and Provost

PART II. EXPLANATION OF NEED (CONFIDENTIAL)

DETAILED EXPLANATION OF WHY ACCESS WITHOUT CONSENT IS DEEMED NECESSARY

Attachment O. Definitions

Compelling Circumstances are circumstances in which failure to act might result in significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of University policies listed in ECP Appendix C, Policies Relating to Access Without Consent, or significant liability to the University or to members of the University community.

Electronic Communications means any transfer of signals, writings, images, sounds, data or intelligence that is, created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several Electronic Communications Systems. For purposes of this Policy, an electronic file that has not been transmitted is not an Electronic Communication.

Electronic Communications Records are the contents of Electronic Communications created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several Electronic Communications Systems or Services. This definition of Electronic Communications Records applies equally to attachments to such records and Transactional Information associated with such records.

Electronic Communications Resources are telecommunications equipment, transmission devices, electronic video and audio equipment, encoding or decoding equipment, computers and computer time, data processing or storage systems, computer systems, servers, networks, input/output and connecting devices, and related computer records, programs, software, and documentation that supports Electronic Communications Services.

Electronic Communications Service Provider means any unit, organization, or staff with responsibility for managing the operation of and controlling individual user access to any part of the University's electronic communications systems and services.

Electronic Communications Systems or Services are any messaging, collaboration, publishing, broadcast, or distribution system that depends on Electronic Communications Resources to create, send, forward, reply to, transmit, distribute, broadcast, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across Electronic Communications network systems between or among individuals or groups, that is either explicitly denoted as a system for Electronic Communications or is implicitly used for such purposes.

Emergency Circumstances means circumstances in which time is of the essence and there is a high probability that delaying action would almost certainly result in Compelling Circumstances.

Faculty means a member of the academic community defined as Faculty by Academic Personnel Manual, APM 110-4 (15).

Holder of an Electronic Communications Record or **Electronic Communications Holder (Holder)** means an Electronic Communications user who, at a given point in time, is in Possession (see definition below) or receipt of a particular Electronic Communications Record, whether or not that Electronic Communications user is the original creator or a recipient of the content of the record.

Except for UCLA Emeritus Faculty and UCLA Emeritus Staff, once an employee separates from the University (s)he is no longer the Holder of the electronic communication records (Section Policy Statement.Except for UCLA Emeritus faculty and UCLA Emeritus staff, and Registered Students, or unless pursuant to an agreement for continuing provision of an Electronic Communications Service (including eligibility for Bruin OnLine services), employees who have separated from the University of California are no longer the Holders of Electronic Communications Records. The University can access these Records without consent and without following the provisions of Section Access without Consent from the point of separation. Nevertheless, when access to such Records is needed, least perusal of contents and the least action necessary to resolve the situation must still be employed.). For students who also are employees, if they use an email account supplied by the University, once they separate from employment, the student maintains Holder status of the account while they are a registered student.

Possession of Electronic Communications Record means an individual is in Possession of an Electronic Communications Record, whether the original record or a copy or modification of the original record, when that individual has effective control over the location of its storage or access to its content. Thus, an Electronic Communications Record that resides on an Electronic Communications server awaiting download to an addressee is deemed, for purposes of this Policy, to be in the Possession of that addressee. Systems administrators and other operators of University Electronic Communications Services are excluded from this definition of Possession with regard to Electronic Communications not specifically created by or addressed to them.

Electronic Communications users are not responsible for Electronic Communications Records in their possession when they have no knowledge of the existence or contents of such records.

Public Record means a record as defined in Business and Finance Bulletin RMP-8, Legal Requirements on Privacy of and Access to Information, and/or the California Public Records Act. Public records include writings or other forms of recording that contain information relating to the conduct of the public's business in materials prepared, owned, used, or retained by the University regardless of physical form or characteristics [California Government Code Section 6252(e)]. Except for certain defined situations, such records are subject to disclosure under the California Public Records Act. For more information regarding the requirements of the Public Records Act, and the University's implementation of that Act, including exemptions from disclosure, see RMP-8.

Substantiated Reason means reliable evidence indicating that violation of law or of University policies listed in the ECP Appendix C, Policies Relating to Access Without Consent, probably has occurred, as distinguished from rumor, gossip, or other unreliable evidence.

Time-dependent, Critical Operational Circumstances means circumstances in which failure to act could seriously hamper the ability of the University to function administratively or to meet its teaching obligations, but excluding circumstances pertaining to personal or professional activities, or to faculty research or matters of shared governance.

Transactional Information is information, including electronically gathered information, needed either to complete or to identify an electronic communication. Examples include but are not limited to: electronic mail headers, summaries, addresses and addressees; records of telephone calls; and IP address logs.

UCLA Authorizing Official is the UCLA administrator identified in Table 1 (Section Prior Authorization) with the authority to approve access to a UCLA Electronic Communications user's Electronic Communications Records without the consent of the user under certain circumstances.

UCLA Emeritus is a retired UCLA Employee, either member of the faculty or staff, upon whom has been conferred formal emeriti status.

UCLA Health includes Ronald Reagan and Santa Monica Medical Centers, Mattel's Children's Hospital, Resnick Neuropsychiatric Hospital, UCLA Health Clinics, UCLA Faculty Group and David Geffen School of Medicine.

University Electronic Communications Record refers to a Public Record in the form of an electronic communications record, whether or not any of the electronic communications resources utilized to create, send, forward, reply to, transmit, distribute, broadcast, store, hold, copy, download, display, view, read, or print the electronic communications record are owned by the University. This implies that the location of the record, or the location of its creation or use, does not change its nature (i) as a University Electronic Communications Record for purposes of this or other University policy, and (ii) as having potential for disclosure under the California Public Records Act.

- Until determined otherwise or unless it is clear from the context, any Electronic Communications Record residing on university-owned or controlled telecommunications, video, audio, and computing facilities will be deemed to be a University Electronic Communications Record for purposes of this Policy. This *would* include personal electronic communications. Consistent with the principles of least perusal and least action necessary and of legal compliance, the University must make a good faith a priori effort to distinguish University Electronic Communications Records from personal communications in situations

relevant to disclosures under the California Public Records Act and other laws, or for other applicable provisions of this Policy.

University Electronic Communications Systems or Services are Electronic Communications Systems or Services owned or operated by the University or any of its sub-units or provided through contracts with the University.