COUNTY OF LOS ANGELES
AGREEMENT|FOR ACCEPTABLE USE
AND CONFIDENTIALITY OF
COUNTY INFORMATION ASSETS

As a County of Los Angeles (County) Workforce Member, and as outlined in Board of Supervisors Policy 6.101 "Use of County Information Assets", I understand and agree:

- That I occupy a position of trust, as such I will use County Information Assets in accordance with countywide and Departmental policies, standards, and procedures including, but not limited to, Board of Supervisors Policy 9.015 "County Policy of Equity" (CPOE) and Board of Supervisors Policy 9.040 "Investigations Of Possible Criminal Activity Within County Government".
- That I am responsible for the security of information and systems to which I have access or to which I may otherwise obtain access even if such access is inadvertent or unintended. I shall maintain the confidentiality of County Information Assets (as defined in Board of Supervisors Policy 6.100 – Information Security Policy).
- That County Information Assets must not be used for:
  - Any unlawful purpose;
  - Any purpose detrimental to the County or its interests;
  - Personal financial gain;
  - In any way that undermines or interferes with access to or use of County Information Asset for official County purposes;
  - In any way that hinders productivity, efficiency, customer service, or interferes with other County Workforce Members performance of his/her official job duties.
- That records, files, databases, and systems contain restricted, confidential or internal use information (i.e. non-public information) as well as Public information. I may access, read or handle Non-public information to the extent required to perform my assigned duties. Although I may have access to Non-public information, I agree to not access such information unless it is necessary for the performance of my assigned duties.
- Not to divulge, publish, share, expose or otherwise make known to unauthorized persons, organization or the public any County Non-public Information. I understand that:
  - I may divulge Non-public Information to authorized County staff and managers as necessary to perform my job duties;
  - I may divulge Non-public Information to others only if specifically authorized to do so by federal, state, or local statute, regulation or court order, and with the knowledge of my supervisor or manager;
  - I may not discuss Non-public Information outside of the workplace or outside of my usual work area;
  - To consult my supervisor or manager on any questions I may have concerning whether particular information may be disclosed.
- To report any actual breach of Information Security or a situation that could potentially result in a breach, misuse or crime relating to County Information Assets whether this is on my part or on the part of another person following proper County and Departmental procedures. I understand that I am expected to assist in protecting evidence of crimes relating to Information Assets and will follow the instructions of, and cooperate, with management and any investigative response team.
- I have no expectation of privacy concerning my activities related to the use of, or access to, County Information Assets, including anything I create, store, send, or receive using County Information Assets. My actions may be monitored, logged, stored, made public, and are subject to investigation, audit and review without notice or consent.
- Not possess a County Information Asset without authorization. Although I may be granted authorization to possess and use a County Information Asset for the performance of my duties, I will never be granted any ownership or property rights to County Information Assets. All Information

Assets and Information is the property of the County. I must surrender County Information Assets upon request. Any Information Asset retained without authorization will be considered stolen and prosecuted as such.

- Not intentionally, or through negligence, damage or interfere with the operation of County Information Assets.
- Neither, prevent authorized access, nor enable unauthorized access to County Information Assets.
- To not make computer networks or systems available to others unless I have received specific authorization from the Information Owner.
  - Not share my computer identification codes and other authentication mechanisms (e.g., logon identification (ID), computer access codes, account codes, passwords, ID cards/tokens, biometric logons, and smartcards) with any other person or entity. Nor will I keep or maintain any unsecured record of my password(s) to access County Information Assets, whether on paper, in an electronic file.
  - I am accountable for all activities undertaken through my authentication mechanisms (e.g., logon identification (ID), computer access codes, account codes, passwords, ID cards/tokens, biometric logons, and smartcards).
- Not intentionally introduce any malicious software (e.g., computer virus, spyware, worm, key logger, or malicious code), into any County Information Asset or any non-County Information Systems or networks.
- Not subvert or bypass any security measure or system which has been implemented to control or restrict access to County Information Assets and any restricted work areas and facilities.
  - Disable, modify, or delete computer security software (e.g., antivirus, antispyware, firewall, and/or host intrusion prevention software) on County Information Assets. I shall immediately report any indication that a County Information Asset is compromised by malware following proper County and Departmental procedures.
- Not access, create, or distribute (e.g., via email, Instant Messaging or any other means) any offensive materials (e.g., text or images which are defamatory, sexually explicit, racial, harmful, or insensitive) on County Information Assets, unless authorized to do so as a part of my assigned job duties (e.g., law enforcement). I will report any offensive materials observed or received by me on County Information Assets following proper County and Departmental procedures.
- That the Internet is public and uncensored and contains many sites that may be considered offensive in both text and images. I shall use County Internet services in accordance with countywide and Departmental policies and procedures. I understand that County Internet services may be filtered, however, my use of resources provided on the Internet may expose me to offensive materials. I agree to hold County harmless from and against any and all liability and expense should I be inadvertently exposed to such offensive material.
- That County electronic communications (e.g., email, instant messages, etc.) created, sent, and/or stored using County electronic communications services are the property of the County. I will use proper business etiquette when communicating using County electronic communications services.
- Only use County Information Assets to create, exchange, publish, distribute, or disclose in public forums and social media (e.g., blog postings, bulletin boards, chat rooms, Twitter, Instagram, Facebook, MySpace, and other social media services) any information (e.g., personal information, confidential information, political lobbying, religious promotion, and opinions) in accordance with countywide and Departmental policies, standards, and procedures.
- Not store County Non-public Information on any Internet storage site except in accordance with countywide and Departmental policies, standards, and procedures.
- Not copy or otherwise use any copyrighted or other proprietary County Information Assets (e.g., licensed software, documentation, and data), except as permitted by the applicable license

agreement and approved by County Department management. Nor will I use County Information Assets to infringe on copyrighted material.

- That noncompliance may result in disciplinary action (e.g., suspension, discharge, denial of access, and termination of contracts) as well as both civil and criminal penalties and that County may seek all possible legal redress.

I HAVE READ AND UNDERSTAND THE ABOVE AGREEMENT:

County Workforce Member's Name	County Workforce Member's Signature
County Workforce Member's ID Number	Date
Manager's Name	Manager's Signature
Manager's Title	Date

COUNTY OF LOS ANGELES – DEPARTMENT OF MENTAL HEALTH
CELLULAR PHONE, SMART PHONE, OR PAGER APPLICATION AGREEMENT

Device Phone Number		Carrier Name	

Employee Last Name:	First Name:	Employee #
Payroll Title:	Office Phone No.:	
Program/Division:	Email Address:	
Contact Person:	Phone No.:	
DMH Service Catalog Request No:	Heat Ticket No:	

Cellular Device Usage Agreement for Cell Phone, Smart Phone, or Pager

I understand and agree that:

Initial each line

	This device is to be used for approved Los Angeles County business only.
	I will not use my device to store, transmit, or receive Protected Health Information (PHI) or Personally identifiable information (PII) without using a CIOB approved technical safeguard.
	In the event the device is lost or stolen, I will immediately notify the DMH Helpdesk at (213) 351-1335 and provide a copy of a law enforcement agency's report along with a Security Incident Report within one (1) business day.
	I will keep all device accessories / packaging and return them with the device to CIOB whenever it is requested of me.
	I will use the case issued to me to protect the device from superficial damage. I could, at my own expense, elect to use another case as long as it provides the same or higher level of protection.
	I am financially responsible for replacement costs of equipment and accessories that are lost, stolen, broken, or damaged due to my negligence, which includes but is not limited to leaving devices unattended/unsecured, submerging them in liquids, etc. The current replacement costs range from $19 up to $281.00.
	If I transfer to a different unit and I am keeping the device, I must submit a new application prior to my transfer.
	I will relinquish this device to the CIOB - Technology Services Division at my manager's request or upon resignation within one (1) business day or the service will be suspended.
	If call forwarding, 411 calls, texting, or downloading appears on my bill, I may be financially responsible.
	Services or features on cellular devices may differ and are made available based on my role and business requirements that I am justified for. DMH reserves the right to cancel any of the services or features on my device at any time. I may be required to return my device if my usage is found unsuitable or no longer in accord with the cellular device justifications listed in LACDMH Policy 1201.01.
	If I am a FLSA covered employee (non-exempt employee), I will only use this equipment during regularly scheduled work hours or during pre-approved overtime.
	I will not alter or make any configuration changes to the cellular device's existing settings because this action may weaken the security of the device and introduce risks of PHI / PII or confidential information compromises and compliance violations.
	For emails that contain PHI / PII or confidential information, I will secure my communications by utilizing DMH Secure Email while following all the guidelines specified in DMH Policy 557.02.
	I will not include any PHI / PII or confidential information in the subject line of my emails.
	I will not include any PHI / client confidential information in my calendar when setting up meetings or appointments.

I understand and agree that:

Initial each line

	Sharing device password is strictly prohibited.
	Downloading, installing, or using applications that are not included in the cellular device is prohibited. All non-standard application installation and use must be pre-approved and installed by CIOB. I will contact the DMH Help Desk if I have a justified business need that requires additional applications.
	Downloading, installing new ringtones, themes, music and non-work related photos, and other materials is prohibited.
	Uploading or posting comments, documents, images, or videos that include sensitive or confidential information to social networking sites, and any non-DMH websites and cloud storage is prohibited. I will contact DMH Help Desk if I have a justified business need that requires this feature.
	Sending or transmitting PHI / PII or confidential data by Enhanced Message Service (EMS) and/or Short Message Service (SMS) such as TEXT Messages, iMessages, Peer-to-Peer Chat, Text Chat, Video Chat, FaceTime, or similar technologies are prohibited. Subsequently, if I ever receive any PHI / PII or confidential data via any of these communication formats, I must contact the sender immediately and make them aware that these types of communications are insecure and must not include PHI / PII or confidential data. I will advise them to permanently remove and delete the message from their mobile device and I will do the same on mine.
	Taking photos or videos that include LACDMH clients, clients' medical information, or structures that can identify clients are strictly prohibited.

Continue to the next page

I have read and understand the following County and Department of Mental Health Policies:

Initial each line

	I have read Board of Supervisors Policy No. 6.101 – Use of the County Information Technology Resources.
	I have read LACDMH Policy No. 1201.01 – Assignment, Use, and Management of Cellular Devices.
	I have read LACDMH Policy No. 1200.05 – Use of LACDMH Technology Resources, Networked Devices, and Information Systems.
	I have read LACDMH Policy No. 557.02 – Appropriate Use of Email for Transmitting Protected Health Information (PHI) and/or Confidential data.

I Received the Following Device and Accessories

☐ Smart Phone	☐ Cellular Phone	☐ Pager	☐ Laptop
☐ Charger / Cable	☐ Hotspot	☐ Headset	☐ Tablet
☐ IMEI	☐ Case/ Holster	☐ ESN	

By signing below, I acknowledge that I have read and understand this Cellular Devices Agreement and agree to abide by it. I recognize that my failure to fulfill these responsibilities, including the knowledge of anyone else using my password, could result in the abuse of County information resources and data and that the County may hold me responsible for such abuse.

Subsequently, I understand that this device is the property of the County of Los Angeles and is provided for authorized use only. There is no expectation of privacy in this system. Any or all uses or access of this device, including all of its data, may be monitored, interrupted, recorded, read, copied, or captured and disclosed in any manner for any lawful or authorized purpose, including disciplinary or civil action and criminal prosecution. Use or access of this device, authorized or unauthorized, constitutes consent to such monitoring, interception, recording, reading, copying or capturing and disclosure.

I further understand that any violation of this agreement may result in disciplinary action up to and including discharge. I also have been informed that failure to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) can result in civil and criminal penalties per 42 USC §1320d-5.

Employee Signature	Print Name	Date

Device and Accessories Returned to CIOB

☐ iPhone	☐ Cellular Phone	☐ Pager	☐ Laptop
☐ Charger / Cable	☐ Hotspot	☐ Headset	☐ Tablet
☐ IMEI	☐ Case/ Holster	☐ ESN	

Returned By (Employee)

Employee Signature	Print Name	Date

Received By CIOB Administration

Employee Signature	Print Name	Date

Authorization to Place Personal and/or Confidential Information on a Portable Computing Device

Department Name **Mental Health**

This Authorization to place (download or input) personal and/or confidential information on a portable computing device (portable computer, portable device, or portable storage media) must be completed for each initial placement (download or input) of the information to each device and be signed by the user of the portable computing device and designated department management in accordance with Board of Supervisors Policy 6.110 - Protection of Information on Portable Computing Devices and Board of Supervisors Policy 3.040 - General Records Retention and Protection of Records Containing Personal and Confidential Information (Note - Policy 3.040 is applicable only for the purpose of providing the definitions of "personal information" and "confidential information'', as referenced in Policy 6.110). However, if the personal and/or confidential information is downloaded from a particular application system to a particular portable computing device, then this Authorization must be completed only for the initial placement (download) of the information on such device, regardless of how often the information is downloaded to such device.

For each initial placement of personal and/or confidential information on each portable computing device, the following steps are required:

1. Provide a description of the portable computing device as indicated below
2. Specify the information to be placed on such device and related information as indicated below
3. Establish an exact copy of the information, preferably on a department computer, to allow for 100% accurate re-creation and audit of the information
4. Encrypt the information during the entire time that it resides on the portable computing device
5. Maintain physical security over the portable computing device during the entire time that the information resides on the device (e.g., the user must maintain physical possession of the device or keep the device secure when unattended)
6. User signature
7. Department management signature

Portable Computing Device Description:

Device Type:	DELL LATITUTE	
Device Serial Number:		
Property Number(Tag#)		
Name of encryption sortware installed:		
Operating System:		

Information Being Placed on the Portable Computing Device:

Purpose of Placement: My job duties may requires me to have access to PHI and if so, I will need a secure place to store the information.

Application system name (if applicabel): IS/IBHIS/MHMIS/MEDS, and in-house developed applications.

Personal and / or confidential information fields: Any field(s) that have been identified as PHI and personal / confidential in nature.

User Agreement and Acknowledgment:

I have read and agree to fully comply with Board of Supervisors Policy 6.110- Protection of Information on Portable Computing Devices and Board of Supervisors Policy 3.040 - General Records Retention and Protection of Records Containing Personal and Confidential Information (note - Policy 3.040 is applicable only for the purpose of providing the definitions of "personal information ' and "confidential information", as referenced in Policy 6.110). I agree to fully comply with all County requirements and directions concerning the above portable computing and personal and / or confidential information.

Name:	Date:
Signature Field:	