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

PORTABLE DEVICE SIGN-OUT / RETURN AGREEMENT

DEVICE			TICKET		ENCRYPTED ON		RAM	
DMH		Service Tag		Express Code			HD SIZE	
	DMH					Aircard		
	DMH					Replacement Device ☐	Shared Device ☐	
	DMH					P.O #		
Mouse ☐	Key Board ☐	Laptop Lock ☐ L ☐ Y	Katie ☐	MHSA ☐	PEI ☐	CGF ☐	Re-Issue ☐	

1. I understand that it is my responsibility to maintain a backup of my stored files located on this portable device
2. Will use this equipment for County business only
3. Will not use the portable device to store, transmit or receive Protected Health Information without the use of a CIOB approved technical safeguard
4. I will immediately notify DMH Helpdesk/Information Security and my supervisor if the device is lost, stolen or missing. I understand that I must complete and submit a Security Incident Report no later than the end of the business day following the incident and provide a copy of law enforcement agency's report
5. Will protect the portable device(s) with a password at all times
6. I will relinquish this equipment to the Technology Services Division at my manager's request or upon resignation or transfer from this Program / Division within one (1) business day of my transfer
7. Will not leave equipment unattended & Will not share my password(s) under any circumstance
8. Will not make copies of vendor software for disclosure or distribution use by any other person, governmental and organization company
9. Will be financially responsible for lost or broken equipment & accessories in the event of neglect or willful damage
10. I have read the Board of Supervisor's Policy No.6.101, Use of County Information Technology Resources
11. I have read the Department of Mental Health's Policy No. 302.14, Network Information Systems Usage.
12. I have read the County of Los Angeles Information Technology Security Guidelines No. 110.01
13. I have read and signed the County of Los Angeles Agreement for Acceptable Use and Confidentiality of County's Information Technology Assets, Computers, Networks, Systems and Data
14. 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.
15. Will any Protected Health Information (PHI) reside on this device? **Yes** ☐ **No** ☐

Accessories:	Carrying Case ☐	Power Adaptor ☐	CD / DVD Drive ☐	Network Cable ☐		
Software						
To		Issued By				

As a LAC-DMH employee, I certify that the agreement and policies listed above have been reviewed with me as of the date indicated below.

Signature		Employee Number		Date	
Address					
Work Phone		Work Cell		Other #	

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:	

Print Form

Laptop Handling Guidelines

Quick Tips in Handling and Securing your Laptop

Treat your laptop like cash!	If you had a wad of money sitting out in a public place, would you turn your back on it – even just for a minute? Would you put it in checked luggage? Leave it on the backseat of your car? Keep a careful eye on your laptop just as you would a pile of cash.
Do not leave your laptop in your car.	Don't leave your laptop on the seat or even locked in the trunk. Locked cars are often the target of thieves.
Limit information stored on your laptop	Store only the minimum amount of information needed to conduct County business on the laptop. Storage of personal or confidential infor mation requires formal written approval as outlined in Board Policy 6.110, Protection of Information on Portable Computing Devices.
Store confidential/personal information on encrypted electronic media	Portable computing devices are stolen more often t hat portable electronic media (CDs, thumb drives, and the like). If you must transport confidential/personal information for County business, consider putting it on encrypted electronic storage media instead of on the computing equipment, and carry the storage media separately.
Secure your laptop when in the office	Secure your laptop by locking it in a docking station, if available, use a security cable, a locked office or locked cabinet. Do not set the laptop on the desk and then walk away for a few minutes. Always secure the laptop in the department approved method.
Secure your laptop when unattended	Attach the laptop with a security cable to something immovable or to heavy piece of furniture when it is unattended. There are devices that sound an alarm when there is unexpected motion or when the computer is moved outside a specified range around you.
Keep it off the floor	No matter where you are in public – at a conference, a coffee shop, or a registration desk – avoid putting your laptop on the floor. If you must put it down, place it between your feet or at least up against your leg, so that you're aware of it.
Do not store your password with your laptop	You should secure your laptop with a strong password, but don't keep the password in the laptop case or on a piece of paper stuck to the laptop
Consider non-traditional bags for carrying your laptop	When you take your laptop on the road, carrying it in a computer case may advertise what's inside. Consider using a suitcase, a padded briefcase or a backpack instead.
Do not store your laptop in checked luggage.	Never store your laptop in checked luggage. Always carry it with you.
Keep track of your laptop when you go through airport screening.	Hold onto your laptop until the person in front of you has gone through the metal detector. Watch for your laptop to emerge from the screening equipment.

Use Encryption	Encrypt entire hard drive as mandated in Board Policy 6.110, Protection of Information on Portable Computing Devices.
Be vigilant in hotels	If you stay in hotels, a security cable may not be enough. Try not to leave your laptop out in your room. Rather, use the safe in your room if there is one. If you're using a security cable to lock down your laptop, consider hanging the "do not disturb" sign on your door.
Record identifying information and mark your equipment.	Record the make, model and serial number of the equipment and keep it in a separate location. Consider having the outside of the laptop case labeled with your organization's contact information and logo.
Backup your files	Make a backup of your files before every trip. In the event that your laptop is lost or stolen, you will still have a copy of your data.
If your laptop is stolen	* Report it immediately to the local authorities * Report it to your Departmental Information Security Officer (DISO), as stated under Board Policy 6.109, Security Incident Reporting

For more information, please read:

* Board of Supervisor Policy 6.109, Security Incident Reporting
* Board of Supervisor Policy 6.110, Protection of Information on Portable Computing Devices

As a LAC-DMH employee, I certify that the agreement and policies listed above have been reviewed with me as of the date indicated below.

Employee Name:	Employee Number:
Employee Signature:	Date: