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:	

Audio & Video Recording Standards

Guidelines for workforce members that have been authorized to conduct Audio & Video Recording

Employee Last Name:	**First Name:**	**Employee #**
Payroll Title:	**Office Phone No.:**	
Program/Division:	**Email Address:**	
Manager/Supervisor:	**Phone No.:**	
Device Brand/Model:	**Usage: Audio ☐ Video ☐**	**Will Include PHI: Yes ☐ No ☐**

Audio & Video Device Usage Agreement

I understand and agree that:

Initial each line

	The use of personal or unapproved Audio or Video Recording devices is strictly prohibited.
	LACDMH workforce members must only use Audio or Video Recording devices that are approved by the HIPAA Privacy and Security Officers or their designees. The device must have been acquired through appropriate procedures
	This Audio or Video Recording equipment is to be used for Los Angeles County business only.
	In the event when the Audio or Video Recording device is lost or stolen; I will immediately notify DMH Helpdesk and provide copy of a law enforcement agency's report along with a Security Incident Report within one business (1) day.
	I will keep all Audio or Video Recording device accessories / packaging and return them with the device to CIOB whenever it is requested of me.
	I am financially responsible for replacement costs of the Audio or Video Recording 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.
	If I transfer to a different unit or division and I am keeping the Audio or Video Recording device, I must contact the HIPAA Privacy and Security Officers and obtain their authorization prior to my transfer.
	I will relinquish this Audio or Video Recording equipment to the CIOB - Technology Services Division at my manager's request or upon resignation within one (1) business day or the phone will be suspended.
	DMH reserves the right to revoke my access to the Audio or Video Recording 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 procedure that I must have followed.
	If I am a FLSA covered employee (non-exempt employee), I will only use this Audio or Video Recording equipment during regularly scheduled work hours or during pre-approved overtime.
	I will not alter or make any configuration changes to the Audio or Video Recording 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.
	All Audio or Video Recordings that may include confidential information such as Protected Health Information must be approved and authorized by both Privacy and Security Officers or their designees.
	Uploading or posting comments, audio files, images or videos that include sensitive or confidential information to social networking sites, and any non-DMH websites and cloud storage is prohibited.
	Taking photos, record audio or film videos that include LACDMH clients, clients' medical information or structures that can identify clients are prohibited.
	This Audio or Video Recording device shall only be utilized and operated in accordance with the instructions and guidelines provided by the Chief Information Office Bureau.

I understand and agree that:

Initial each line

	Sharing device password with unauthorized or non DMH workforce is strictly prohibited.
	The recording devices must be secured in a locked storage cabinet when not in use. All equipment must be checked in and out, time stamped and recorded on a log sheet maintained by a designated staff.
	I shall not leave audio and video equipment unattended. Workforce members must safeguard and protect the data stored on the devices at all times.
	I shall not connect the recording device, upload or download any Audio or Video recorded files onto a non-DMH computer or equipment.
	Once recording session is complete, the recoded file must be uploaded to a CIOB approved secure server or a CIOB approved Encrypted portable storage. If the storage is shared or accessible by others, the workforce must consider additional caution for others who can access, view, alter or delete the recordings.
	After the successful transfer of the recorded file, any resident data, Audio or Video recordings must be immediately removed and deleted from the recorder's internal storage. If the device uses removable SD Cards, they must be wiped clean and formatted. No data shall reside on the recorders when the device is not in use.
	I shall not name the data file to include identifiable words such as client name, last name, MIS number, SS number. Always use general names such as session taped on "date" etc.
	Transporting and delivery of any audio or video recording must be through a CIOB-approved method.
	I shall not Mail, distribute or transmit recorded audio/video sessions unless data is pre-encrypted using CIOB approved encryption method.
	Any audio or video recordings received from non-DMH individuals and sources must be inspected and reviewed by DMH Privacy and Security Officers or their respected designees.
	In the event when a recorded file is no longer needed, it must be sanitized in a format consistent with policy 554.01 – LACDMH Device/Media Controls. Memory cards & portable media must be returned to CIOB for proper destruction.
	A malfunctioning or defective recording device or one that is no longer needed must be discarded in accord to policy 554.01 – LACDMH Device/Media Controls. The device must be returned to CIOB for appropriate disposal.

Each authorized workforce member is required to acknowledge and agree with the following guidelines prior to utilize or operate the Audio and Video device by signing this document.
The document must be placed in the employee facility personnel folder and maintained by the manager.
A copy of this document may be given to the workforce member to be used as a referenced checklist.

By signing below I acknowledge that I have read and understand this Audio & Video Standards and agree to abide by it.
I recognize that my failure to fulfill these responsibilities, including the knowledge of anyone unauthorized 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. 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**
Approving Manager Signature	**Print Name**	**Date**

Caution: Please Read This First

NOTE: The Philips Audio Recorders are pre-configured, Pin and Password Protected, and Encrypted. Please do not guess the device's 4 digit Pin. **5 incorrect entries** will result to a device lock which can only be restored by the manufacture. Please contact your Project Lead or Coordinator for the Device Access PIN and Decrypting Passcode. If your Project Lead is unavailable to assist, please contact DMH Helpdesk at (213) 351-1335.
To unlock the audio recorder, please use the device's (+) and (-) buttons to increase or decrease the digits and left or right function keys to navigate and enter the 4 digit Pin.

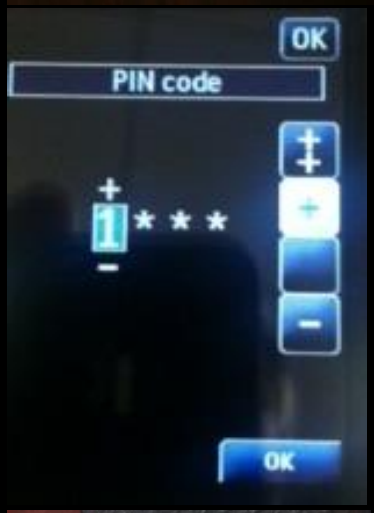
NOTE: To meet compliance with LAC-DMH Federal Requirements; file modification, alteration and deletion has been disallowed directly from the device. The above mentioned functions can only be performed when the operator connects the audio recorder to a DMH workstation using the provided USB cable; navigate to the designated drive letter and folder; select the desired file(s); and then move, copy or delete it from the recorder.

NOTE: Special software and a Master Passcode are required in order to decrypt and access the encrypted audio recordings when using a computing device. Please consult with your Project's Lead or Coordinator to ensure that the Philips SpeechExec Pro Dictate Application and Master Passcode were accordingly distributed and delivered to one's authorized to access your recorded audio files.

Operating Instructions for Philips Audio Recorders

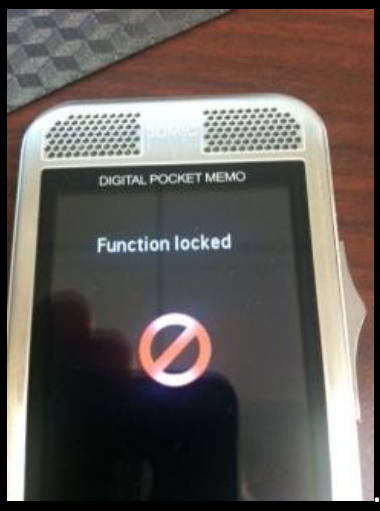
1. **Power on the fully charged Philips Audio Recorder by sliding the power button on the side of the device.**

2. **To unlock the audio recorder, please use the device's (+) and (-) buttons to increase or decrease the digits and left or right function keys to navigate and enter the 4 digit Pin.**
   Warning: Please do not guess the device's 4 digit Pin. 5 incorrect entries will result to a device lock which can only be restored by the manufacture.
   The 4 digit pin can be obtained from your Project Manager /Coordinator. If your Project Lead is unavailable to assist, please contact DMH Helpdesk



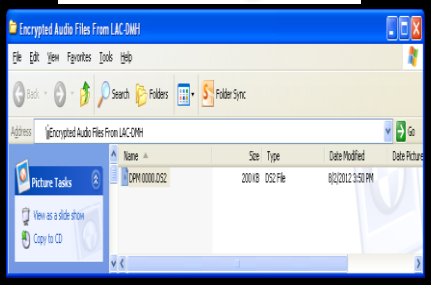
3. **Move the control slider to record, stop, and play or rewind positions to operate the desired feature.**

4. **To meet compliance with LAC-DMH Federal Requirements; any intentional or accidental audio segment insertion, alteration, modification, and deletion has been disallowed directly from the device.**
   Note: The above mentioned functions can only be performed when the operator connects the audio recorder to a workstation using the provided USB cable; navigate to the designated drive letter and folder; select the desired file(s); and then move, copy or delete it from the recorder.

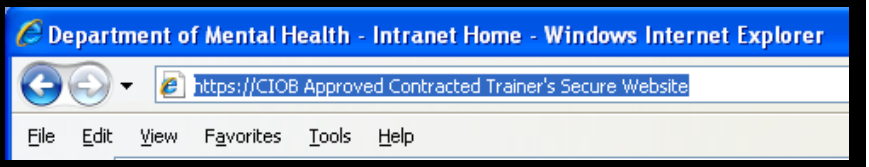


5. **Connect Audio recorder to the computer with the included USB cable.**

6. **Verify your Audio recorder's connection by observing the appearance of a new drive letter in "My Computer".**

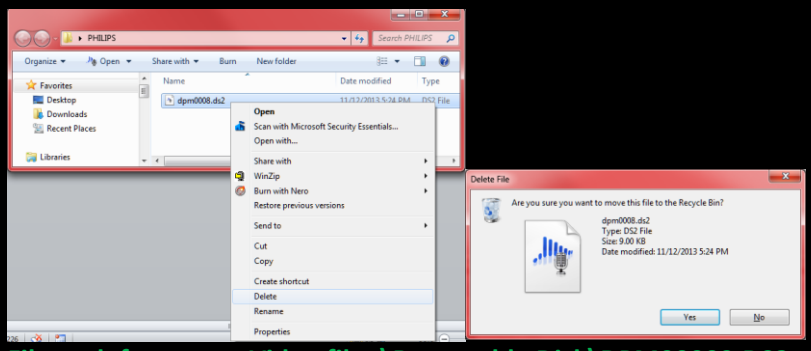


7. **Follow your Project Manager's or Coordinator's provided procedure to sign-on to the LAC-CIOB approved website specifically for the audio file transmission. Browse, select and upload the recorded audio file to the secure website.**
   Note: In order to prevent a data breach due to an accidental sensitive information compromise the audio recorder shall never contain any file after a successful upload.



8. **Delete the audio file from the device immediately as described below:**

   Upon a successful upload of the audio file to the approved website, access the drive letter specific to the audio recorder in "My Computer", navigate to the device folder that contains the audio file, right click and select the file on the device. Select delete from menu choices, confirm and delete the file.



File path for source Video file: \Removable Disk\DPM00000.DS2

9. **Power off and disconnect the Audio Recorder and the USB Cable from the workstation.**

10. **Refer to the Audio & Video Recording Standards for appropriate storage, transportation, handling, and submission of Encrypted Contents. Never leave the device unattended. You will be held responsible for it.**

11. **A special software and a Master Passcode are required in order to decrypt and access the encrypted audio recordings when using a computing device. Please consult with your Project's Lead or Coordinator to ensure that the Philips SpeechExec Pro Dictate Application and the Master Passcode were accordingly distributed and delivered to one's authorized to access and listen to your recorded audio files.**