COUNTY OF LOS ANGELES
Public Health

CYNTHIA A. HARDING, MPH
Interim Director

JEFFREY D. GUNZENHAUSER, MD, MPH
Interim Health Officer

Division of HIV and STD Programs
Mario J. Pérez, Director
600 South Commonwealth Avenue, 10th floor
Los Angeles, California 90005
TEL (213) 351-8000 • FAX (213) 387-0912

www.publichealth.lacounty.gov

BOARD OF SUPERVISORS

Hilda L. Solis
First District

Mark Ridley-Thomas
Second District

Sheila Kuehl
Third District

Don Knabe
Fourth District

Michael D. Antonovich
Fifth District

April 10, 2015

Dear Provider of HIV Care and Treatment Services:

PROGRAM GUIDANCE 2015.02: USE AND ACCESS TO CASEWATCH

Purpose

The Division of HIV and STD Programs (DHSP) uses Casewatch Millennium ®, developed by Automated Case Management Systems, Inc. (ACMS), as the multi-user database system to track and report on the delivery of HIV care and treatment programs and services funded under the local Ryan White Program (RWP). This program guidance is to clarify DHSP's expectations on the use of Casewatch, as well as the process that contracted providers shall follow for requesting approval for staff (end-user(s)) to the data system.

Uses of Casewatch

As previously noted, Casewatch is used to track and report on various aspects of HIV care and treatment service delivery including but not limited to:

1. collecting and documenting consumer-level protected personal health information (PHI) such as consumer eligibility for RWP-supported services, health status, assessments and acuity, and treatment plans;
2. coordinating service delivery;
3. tracking and reporting on services accessed by and delivered to eligible consumers;
4. tracking and reporting on various performance measures; and
5. generating invoices for various programs and services.

Safeguarding PHI in Casewatch

As a repository of PHI, the use of Casewatch is governed by a variety of federal, state, and County laws, codes, rules and regulations. These include but are not limited to the federal Health Insurance Accountability Portability Act (HIPAA); California Penal Code 502(c)-Comprehensive Computer Data Access and Fraud Act; the Los Angeles County Information Technology Assets, Computers, Networks, Systems and Data policy; as well as other state health and safety regulations specific to PHI related to HIV, other STDs, substance abuse and mental health.

Casewatch Data Security

While Casewatch is HIPAA-compliant, ensuring the protection of PHI is an ongoing and shared responsibility. DHSP expects that all contracted providers train all staff on all applicable rules and regulations regarding PHI and the use of Casewatch. The Los Angeles County Department of Public Health (DPH), DHSP, and ACMS work collaborative to closely monitor proper access to and use of Casewatch and the information it contains, and will take corrective actions when potential threats to the data system and the PHI within are reported or detected.

It is the contracted providers' responsibility to ensure that its end-users are fully trained on all laws, policies, rules, and regulations applicable the handling of PHI and the use of Casewatch. It is also the contractors' responsibility to ensure that their end-users use sound judgment in accessing, safeguarding information and computer equipment from accidental or deliberate unauthorized access, tampering, distribution or destruction. Misuse, abuse or negligence on the part of end-users is unacceptable and will be cause for modification or termination of access and/or discipline for non-compliance with DHSP's policies and other applicable laws, rules, and regulations.

DHSP will take corrective and disciplinary actions when Casewatch end-users fail to comply with applicable policies and procedures as outlined by the HIPAA privacy rule and security rule (http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html), or engage in any unauthorized or inappropriate behavior that undermines the privacy or security of PHI. Depending on the circumstances, disciplinary measures may include verbal and written warnings, requests for re-training, a ninety-day (90) suspension of or termination of Casewatch access rights.

Contractors must inform DHSP in writing of any improprieties in the handling of PHI or Casewatch access. If contractors identify an issue or situation that warrants attention, the respective DHSP program manager shall be contacted.

Requesting Approval to Access Casewatch

DHSP will consider requests from contracted providers to grant access to Casewatch to new and current employees, as well as certain interns and temporary/contract staff directly or indirectly involved in the delivery of HIV care and treatment services funded as part of the local RWP. Direct involvement means that the employee, intern or temporary/contract staff person is listed on a DHSP-approved budget to provide a service component or carry a function related to the contract such as eligibility determination, service delivery and care coordination, program supervision, data entry, and generation of service reports and invoices. Indirect involvement means that the employee, intern or temporary/contract staff person is not listed on a DHSP-approved budget but he or she carries a function related to the contract such as quality management, program supervision/coordination, data entry, or generation of service reports and invoices.

DHSP will not consider requests for individuals that do not meet the criteria above. In addition, DHSP will not approve grant access to Casewatch to volunteers, temporary/contract staff scheduled to serve less than three months at the agency, or interns not previously approved by DHSP to deliver services under any of its contracts with the requesting community or County partner.

In order to request access to Casewatch, providers must submit an application packet consisting of:

1. a letter listing the name(s), job title(s)/duties of the employee(s), intern(s) or temporary/contract staff for whom access is being requested;
2. the resume(s) and relevant credentials (e.g. medical/clinical licenses, certifications, etc.) for each person listed on the application letter; and

3. completed and signed copies of the forms below (see attachments) for each person listed on the letter:
    a. Casewatch Millennium® User Request Form;
    b. Casewatch Millenium® Security and Confidentiality Attestation; and
    c. County of Los Angeles, Downey Data Center Registration for Contractors/Vendors.

Application packets must be submitted to the attention of: Carlos A. Vega-Matos, Chief, Care Services, Division of HIV and STD Programs, 600 South Commonwealth Avenue, Los Angeles California 90005. Providers are encouraged to submit the completed packets electronically to the following e-mail address: DHSP-ChiefofCS@ph.lacounty.gov.

Contractors are responsible for notifying DHSP of new end-users promptly and submit the required documents within seven (7) business days from the start or separation of contract-related duties. DHSP staff will review the application packets and approve or deny the request within seven (7) business days from receipt at DHSP, assuming the application packets are completed and signed as required. Contractors will be provided written communication of DHSP's final determination. Approved requests for Casewatch access will be referred to the DHSP Program Evaluation and Data Management team to coordinate the issuance of Casewatch end-user accounts, and VPN tokens (when required). Both the provider and ACMS will be provided with the Casewatch end-user account information. This part of the process may take up to fourteen (14) business days. The entire approval process may take up to twenty (21) days from the date of receipt of the application. Upon receipt of the end-user account information, providers should contact ACMS to schedule the relevant Casewatch trainings by calling 323-460-7700 x19.

Reinstatement of Casewatch User Access

Contractors may request the reinstatement of access to Casewatch for end-users whose access rights were suspended for violations to applicable of applicable policies, laws, rules and regulations, account inactivity of six (6) months or more, changes in job duties, or other mitigating circumstances. To this end, contractors shall follow the process outlined under Requesting Approval to Access Casewatch. DHSP will review the application and provide a written confirmation of its decision within twenty-one (21) business days. Please note that DHSP will not reinstate access rights for end-users who incur on a second violation of applicable policies, laws, rules and regulations.

A copy of this Program Guidance and required forms can be found in the 'For Contractors' section of the DHSP's website: http://www.publichealth.lacounty.gov/dhsp/.

If you have any questions or need additional information, please contact your designated DHSP program manager.

Very truly yours,

Carlos Vega-Matos, Chief
Care Services

CVM:rb

c: Mario J. Perez (DHSP)
Mike Janson (DHSP)
Lisa Klein (DHSP)
ACMS
Chron

COUNTY OF LOS ANGELES
Public Health

Casewatch User Request Form

Add New User ☐ Reinstate a Previous Casewatch User ☐ Date:_____

User Name: _____ Title: _____

Agency:_____ Site Address:_____

City: _____ Zip Code: _____

Telephone: _____ Email: _____

DHSP Service Category(ies) AND Contract Number(s)(**List All**)_____

_____

Is staff on the DHSP budget for the requested service categories & contracts listed above? ☐ Yes ☐ No

How will this staff use Casewatch? ☐ User's Own Direct Services ☐ Invoices

☐ Reports/QM/Administrative ☐ Data Entry Staff (**Entering Data for other Staff's Direct Services**)
*For whom? _____

Is the above staff replacing another Casewatch User? ☐ Yes ☐ No If yes, whom?

Name _____ Title _____

Please note that the staff being replaced will be deactivated from Casewatch.

Previous Casewatch Users: Reason account was deactivated: ☐ Non-Use ☐ Violation of Policy ☐ Other

Explanation of above: _____

_____

List agency and service(s) previously authorized for_____

_____

Approved by: Supervisor Name and Title: _____ Signature: _____

Telephone: _____ Email: _____

DHSP USE ONLY Budget information above has been reviewed & verified? ☐ Yes ☐ No
Casewatch Access approved? ☐ Yes, Indefinitely ☐ Yes, Temporary_____ ☐ No

If no, provide explanation: _____

Program Manager:_____ Signature: _____ Date:_____

COUNTY OF LOS ANGELES
Public Health

Casewatch Millennium® Security and Confidentiality Attestation

Contractor Information:

Agency/Provider Name: _____

Site (if applicable): _____

Address: _____

City: _____ Zip Code: _____

By signing this form as an authorized agency representative, I am certifying that: 1) the user identified below is an employee of the agency who understands the security and confidentiality requirements of the Health Insurance Portability and Accountability Act (HIPAA), the agency, and Casewatch protocol; and, 2) their job requires the level of access to Casewatch Millennium® I have indicated below.

Agency Authorization (please **print** name clearly): _____

_____ _____

Signature *Date*

User Information (Please print clearly):

First Name: _____ Last Name: _____

Email: _____ Phone: _____

Job Title: _____

DHSP Contract # _____

By signing this form as an employee of the above Agency/Provider, I am attesting that I have been trained in the confidentiality requirements of HIPAA and that I will follow my Agency's/Provider's guidelines as well as Casewatch protocol pertaining to data security and confidentiality. I will not under any circumstance share my user account information or password and I will report any potential or real security or confidentiality breach to my supervisor and DHSP immediately. I understand that failure to comply with DHSP security and confidentiality protocols and HIPAA regulations may result in a 90-day suspension of my use of Casewatch and a HIPAA violation report.

_____ _____

Employee Signature *Date*

Send form to DHSP Casewatch User Support at DHSPITSupport@ph.lacounty.gov

DHSP Data Management Authorization:

_____ _____ _____

Printed Name Signature Date

Level of access:

ACMS Use Only:

Date Received: _____ Received by: _____

Date of Training: _____ Trained by: _____

User ID Assigned: _____ Date Assigned: _____

Activation Date: _____ Activated by: _____

Level of Access: _____

Revocation Information:

Deactivation Date: _____ Deactivated by: _____

Revised: 10/09/2014

First Name:

Last Name:

Print Form

LOS ANGELES COUNTY ISD INTERNAL SERVICES

COUNTY OF LOS ANGELES
DOWNEY DATA CENTER REGISTRATION
For Contractors/Vendors

PROFILE INFORMATION — print or type completing boxes 1 – 9

(1) DATE OF REQUEST

(2) TYPE OF REQUEST (Check One) ☐ REPLACE LOST/STOLEN SECUREID TOKEN ☐ ADD NEW LOGON ID ☐ CHANGE LOGON ID ACCESS ☐ DELETE LOGON ID

(3) CONTRACT OR VENDOR NUMBER

(4) LAST NAME, FIRST NAME MI

(5) E-MAIL ADDRESS

(6) COMPANY/ORGANIZATION NAME

(7) COORDINATING L.A. COUNTY DEPARTMENT NAME / NUMBER

(8) WORK MAILING ADDRESS (STREET, CITY, STATE, ZIP)

(9) WORK PHONE NUMBER

IBM DATA CENTER ACCESS — complete each area for required access, as defined by L.A. County management

(10) LOGON ID

(11) 2-DIGIT MAJOR GROUP CODE

(12) 2-DIGIT LSO GROUP CODE

☐ **TSO ACCESS** — check box and complete for required access, as defined by L.A. County management. Asterisks are optional data.

(13) 2-DIGIT TSO GRP CODE

(14) SUB-GROUP 1 *

(15) SUB-GROUP 2 *

(16) SUB-GROUP 3 *

☐ **ONLINE ACCESS** — check box and complete for required access, as defined by County management. Asterisks are optional data.

(17) SYSTEM APPLICATION

(18) GRP NAME / NATURAL PROFILE

(19) OLD GRP/NATURAL PROFILE *

DMV/JAI/APS APPLIATION COORDINATORS ONLY

APS A/O: _____

DMV SYSTEM CODE: _____

JAI SYSTEM LOCATION: _____

UNIX ENVIRONMENT ACCESS — complete for required access, as defined by L.A. County management.

(20) TYPE OF REQUEST (Check One) ☐ ADD NEW LOGON ID ☐ CHANGE LOGON ID ACCESS ☐ DELETE LOGON ID

(21) LOGON ID

(22) APPLICATION

(23) ACCESS GROUP

(24) ACCOUNT NUMBER

SECURID REMOTE ACCESS — complete as defined by L.A. County mgnt., e-mail address is required, see box #5

(25) BILLING ACCOUNT NUMBER for SecurID Token: _____

(26) DEVICE TYPE: KEY FOB

☐ **VPN**

SECURITY STATEMENT

Before connecting to the County network you must install anti-virus software, and stay up-to-date with definitions, Microsoft patches (critical and security) and service packs. A Firewall, either a hardware firewall or personal firewall software, is required for those using broadband Internet access (DSL, ISDN, cable modem, etc.). You agree not to share your logon id, password and SecurID passcode with others.

SIGNATURES — each signature entry must be completed in full.

Your signature indicates that you have read and will comply with the above **security statement.**

(27) CUSTOMER'S SIGNATURE:

(28) COUNTY DEPARTMENT MANAGER'S SIGNATURE

(29) PHONE #

(30) PRINT COUNTY DEPARTMENT MANAGER'S NAME

(31) DATE

(32) ISD/APPLICATION COORDINATOR'S SIGNATURE

(33) PHONE #

(34) PRINT ISD/APPLICATION COORDINATOR'S NAME

(35) DATE

WARNING: FAILURE TO FULLY COMPLETE & SIGN THIS FORM WILL CAUSE A DELAY IN PROCESSING.

You may submit completed registration form to ISDRegistration@isd.lacounty.gov or ISD Registration office at 9150 E. Imperial Hwy, Downey, CA 90242 Mail Stop # 29 to **process**.

For any questions related to registration please call (562) 658-1881.

Revised: November 2011

Downey Data Center Registration Instructions

For Contractors/Vendors

Profile Information — print or type

1. Mandatory. Enter the current date.
2. Mandatory. Check appropriate type of request.
3. Mandatory. Enter your contract or vendor number.
4. Mandatory. Print your last name, first name and middle initial.
5. Mandatory. Enter your e-mail address.
6. Mandatory. Enter your company/organization name.
7. Mandatory. Enter the coordinating L.A. County department name or number.
8. Mandatory. Enter your complete business mailing address.
9. Mandatory. Enter your complete telephone number.

New logon ids will be created as follows:

Contractor/Vendor LOGON ID will be assigned and you will be notified by phone (e.g. Cxxxxxx).

IBM Data Center Access

10. Mandatory. Enter your existing logon id. If this is a new request, your logon id will be assigned as described above.
11. Mandatory. Enter the two-digit department major group code, as defined by L.A. County management.
12. Mandatory. Enter the two-digit local security group code, as defined by L.A. County management.

TSO Access — check box if this request applies to TSO access

13. Mandatory. Enter the two-digit identifier of your TSO group, as defined by L.A. County management.
14. Optional. Enter the two-character identifier, as defined by L.A. County management.
15. Optional. Enter the two-character identifier, as defined by L.A. County management.
16. Optional. Enter the two-character identifier, as defined by L.A. County management.

Online Access — check box if this request applies to online access

17. Mandatory. Enter each CICS online or IMS system application required for access, as defined by L.A. County management.
18. Mandatory Enter the group name for each system application, as defined by L.A. County management.
19. Optional. Enter the old Natural group/profile name.

UNIX Environment Access — complete for required access as defined by L.A. County management

20. Mandatory. Check appropriate type of request.
21. Mandatory. Enter your existing Logon ID. If this is a new request, your logon id will be assigned as described above.
22. Mandatory. Enter the application you require for access, as defined by L.A. County management.
23. Mandatory. Enter your UNIX access group.
24. Optional. Enter a valid 11-digit billing account number.

SecurID Remote Access — complete for required access as defined by L.A. County management.

25. Mandatory. Enter a valid L.A. County 11-digit billing account number.
26. Mandatory. Check box for device type.

    VPN customers must check the box and indicate compliance. Anti-virus software and stay up-to-date with definitions, patches and service packs applies to everyone. A Firewall, either a hardware firewall or personal firewall software, is required for those using broadband Internet access (DSL, ISDN, cable modem, etc.).

Signatures — original signatures are required

27. Mandatory. Your signature indicates that you have read and will comply with the security statement.
28. – 31. Mandatory. Enter signature, phone # and date of authorizing L.A. County department manager (sign and print).
32. – 35. Mandatory. Enter signature, phone # and date of ISD manager or application coordinator (sign and print).

COUNTY'S INFORMATION TECHNOLOGY ASSETS, COMPUTERS, NETWORKS, SYSTEMS AND DATA

As a Los Angeles County employee, contractor, vendor or other authorized user of County Information Technology (IT) assets including computers, networks, systems and data, I understand that I occupy a position of trust. I will use County IT assets for County management approved business purposes only and maintain the confidentiality of County's business and Citizen's private data. As a user of County's IT assets, I agree to the following:

1. Computer crimes: I am aware of California Penal Code 502(c) - Comprehensive Computer Data Access and Fraud Act (attached). I will immediately report any suspected computer misuse or crimes to my Management.

2. Security access controls: I will not subvert or bypass any security measure or system which has been implemented to control or restrict access to computers, networks, systems or data. I will not share my computer identification codes (log-in ID, computer access codes, account codes, ID's, etc.) or passwords.

3. Approved business purposes: I will use the County's Information Technology (IT) assets including computers, networks, systems and data for County management approved business purposes only.

4. Confidentiality: I will not access or disclose any County program code, data, information or documentation to any individual or organization unless specifically authorized to do so by the recognized information owner.

5. Computer virus and malicious code: I will not intentionally introduce any computer virus, worms or malicious code into any County computer, network, system or data. I will not disable or delete computer virus detection and eradication software on County computers, servers and other computing devices I am responsible for.

6. Offensive materials: I will not access or send any offensive materials, e.g., sexually explicit, racial, harmful or insensitive text or images, over County owned, leased or managed local or wide area networks, including the public Internet and other electronic mail systems, unless it is in the performance of my assigned job duties, e.g., law enforcement. I will report to my supervisor any offensive materials observed by me or sent to me on County systems.

7. Public Internet: I understand that the Public Internet is uncensored and contains many sites that may be considered offensive in both text and images. I will use County Internet services for approved County business purposes only, e.g., as a research tool or for electronic communication. I understand that the County's Internet services may be filtered but in my use of them I may be exposed to offensive materials. I agree to hold the County harmless should I be inadvertently exposed to such offensive materials. I understand that my Internet activities may be logged, are a public record, and are subject to audit and review by authorized individuals.

8. Electronic mail and other electronic data: I understand that County electronic mail (e-mail), and data, in either electronic or other forms, are a public record and subject to audit and review by authorized individuals. I will comply with County e-mail use policy and use proper business etiquette when communicating over e-mail systems.

9. Copyrighted materials: I will not copy any licensed software or documentation except as permitted by the license agreement.

10. Disciplinary action for non-compliance: I understand that my non-compliance with any portion of this Agreement may result in disciplinary action including my suspension, discharge, denial of service, cancellation of contracts or both civil and criminal penalties.

CALIFORNIA PENAL CODE 502(c) - "COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT"

Below is a section of the "Comprehensive Computer Data Access and Fraud Act" as it pertains specifically to this Agreement. California Penal Code 502(c) is incorporated in its entirety into this Agreement by reference and all provisions of Penal Code 502(c) apply. For a complete copy, consult the Code directly at website www.leginfo.ca.gov/.

502.(c) Any person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongly control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies or makes use of any data from a computer, computer system, or computer network, or takes or copies supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network is in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

I HAVE READ AND UNDERSTAND THE ABOVE AGREEMENT:

Employee's Name	Employee's Signature	Date
Manager's Name	Manager's Signature	Date