ISACA®

Trust in, and value from, information systems

San Francisco Chapter

Session Number – G24

Responding to a Data Breach and Its Impact

Karen Johnson

Chief Deputy Director

California Department of Health Care Services

Outline

- PCI and PCH
- Breach Incident
- Incident Response
- Lessons Learned
- DHCS Data Release Policy

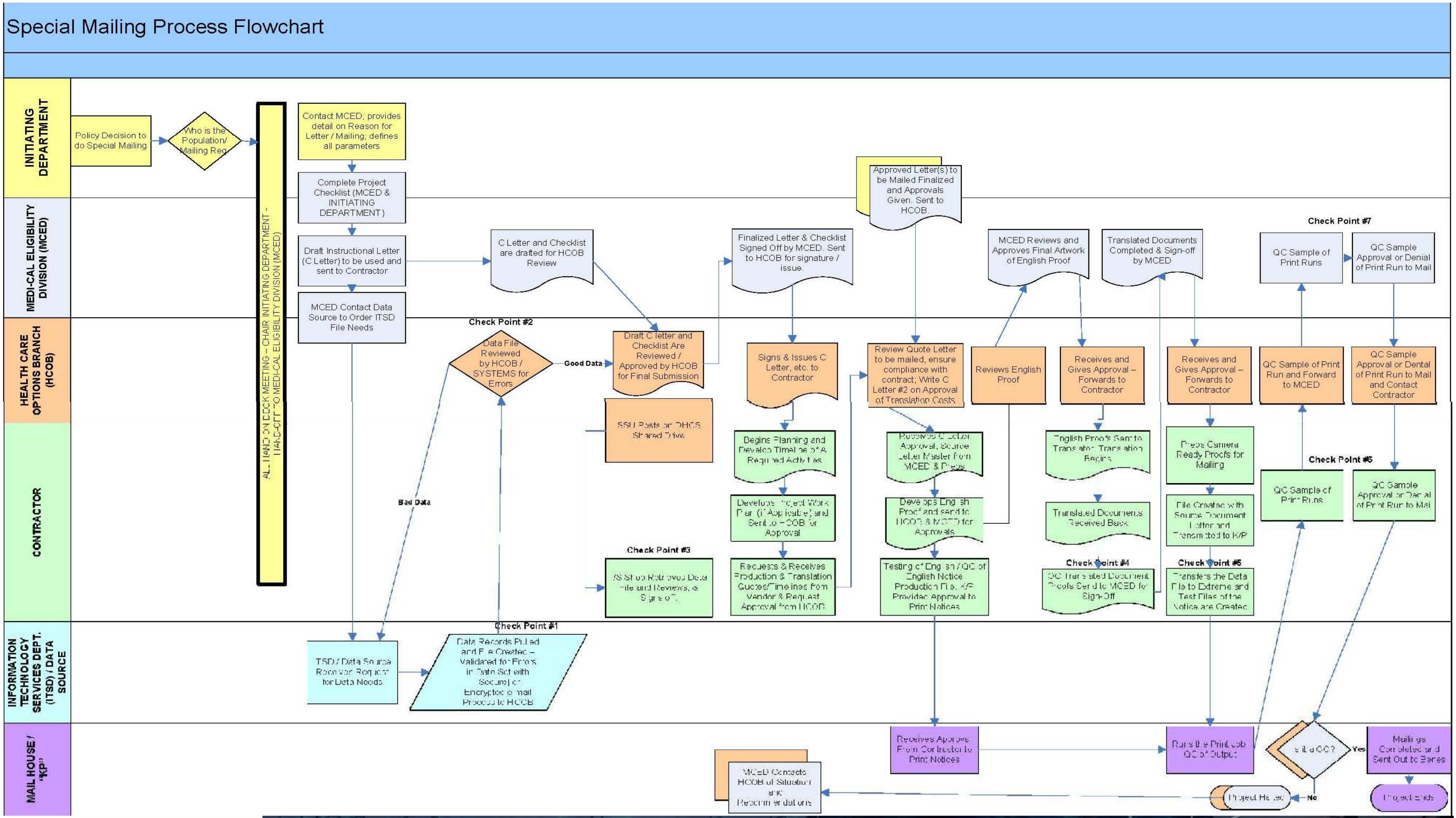
PCI and PCH that DHCS Controls

- The California Department of Health Care Services (DHCS) is responsible for the privacy and security of Personal Confidential Information (PCI) and Protected Health Information (PHI).

- Confidential data includes the following:

  1. PHI,
  2. Personal Information (PI),
  3. or any other data deemed confidential by DHCS

Special Mailing Process Flowchart



Special Mailing Process Flowchart

INITIATING DEPARTMENT

Policy Decision to do Special Mailing

Who is the Population/ Mailing Req

Contact MCED; provides detail on Reason for Letter / Mailing; defines all parameters

ALL HAND ON DECK MEETING – CHAIR INITIATING DEPARTMENT - HAND-OFF TO MEDI-CAL ELIGIBILITY DIVISION (MCED)

MEDI-CAL ELIGIBILITY DIVISION (MCED)

Complete Project Checklist (MCED & INITIATING DEPARTMENT)

Draft Instructional Letter (C Letter) to be used and sent to Contractor

MCED Contact Data Source to Order ITSD File Needs

C Letter and Checklist are drafted for HCOB Review

Finalized Letter & Checklist Signed Off by MCED. Sent to HCOB for signature / issue.

Approved Letter(s) to be Mailed Finalized and Approvals Given. Sent to HCOB.

MCED Reviews and Approves Final Artwork of English Proof

Translated Documents Completed & Sign-off by MCED

Check Point #7

QC Sample of Print Runs

QC Sample Approval or Denial of Print Run to Mail

HEALTH CARE OPTIONS BRANCH (HCOB)

Check Point #2

Data File Reviewed by HCOB / SYSTEMS for Errors

Good Data

Draft C letter and Checklist Are Reviewed / Approved by HCOB for Final Submission

Signs & Issues C Letter, etc. to Contractor

Review Quote Letter to be mailed, ensure compliance with contract; Write C Letter #2 on Approval of Translation Costs

Reviews English Proof

Receives and Gives Approval – Forwards to Contractor

Receives and Gives Approval – Forwards to Contractor

QC Sample of Print Run and Forward to MCED

QC Sample Approval or Dental of Print Run to Mail and Contact Contractor

CONTRACTOR

Bad Data

SSU Posts on DHCS Shared Drive

Begins Planning and Develop Timeline of A Required Activities

Develops Project Work Plan (if Applicable) and Sent to HCOB for Approval

Check Point #3

IS Shop Retrieves Data File and Reviews, & Signs off.

Requests & Receives Production & Translation Quotes/Timelines from Vendor & Request Approval from HCOB

Receives C Letter Approval, Source Letter Master from MCED & Preps

Develops English Proof and send to HCOB & MCED for Approvals

Testing of English / QC of English Notice Production File. K/P Provides Approval to Print Notices

English Proofs Sent to Translator. Translation Begins

Translated Documents Received Back

Check Point #4

QC Translated Document Proofs Send to MCED for Sign-Off

Preps Camera Ready Proofs for Mailing

File Created with Source Document Letter and Transmitted to K/P

Check Point #5

Transfers the Data File to Extreme and Test Files of the Notice are Created

Check Point #6

QC Sample of Print Runs

QC Sample Approval or Denial of Print Run to Mail

INFORMATION TECHNOLOGY SERVICES DEPT. (ITSD) / DATA SOURCE

TSD / Data Source Receives Request for Data Needs

Check Point #1

Data Records Pulled and File Created – Validated for Errors in Data Set with Secure [illegible] or Encrypted e-mail Process to HCOB

MAIL HOUSE / "KP"

MCED Contacts HCOB of Situation and Recommendations

Receives Approval From Contractor to Print Notices

Runs the Print Job QC of Output

Still a QC?

Yes

No

Mailings Completed and Sent Out to Benes

Project Halted

Project Ends

Breach Incident – February 1, 2010

- Problem Statement

  Disclosure of personal information during a mass mailing to Medi-Cal beneficiaries

- What?

  Social security numbers were printed on the outside of 49,352 envelopes that were sent via U.S. Postal Service

- Cause?

  Failure to follow data release process resulted in the data breach

Notifications

- Breach notification on February 4, 2010
- Minimize risk of SSN exposure, individual notifications must be done as soon as possible
- First individual notification letters were sent February 6th; by February 9th all letters in thirteen threshold languages had been sent
- Key third parties (providers & associations) were called; 2nd letters were sent on February 10th
- Sample individual letter was posted on DHCS Web site and a press release was issued
- CMS, SSA and other state agencies were notified of the breach as required by breach laws and state policy

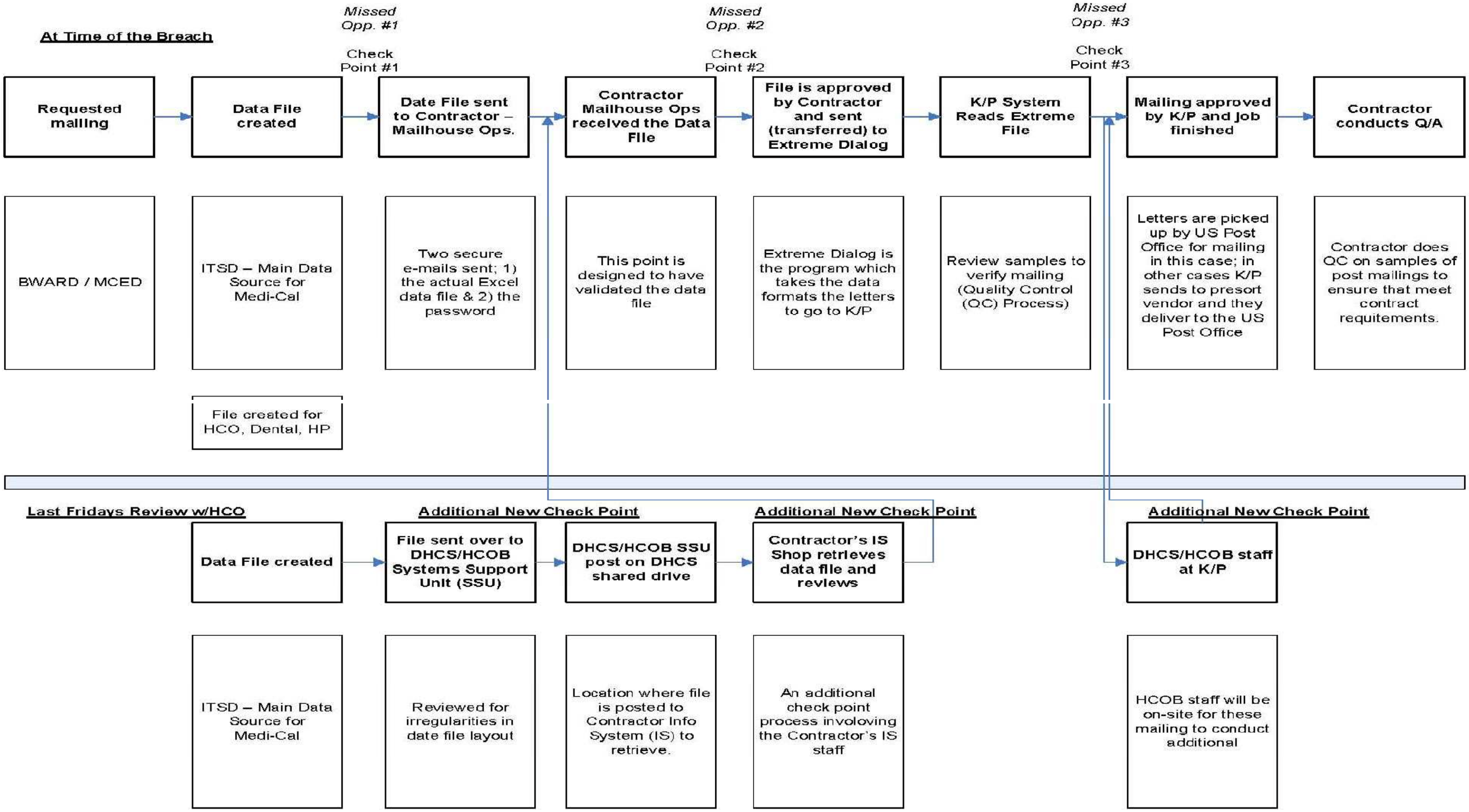
Mitigation of Potential Harm

- DHCS arranged for one-year free credit monitoring services for impacted individuals, which included:
  - Free credit reports;
  - Automatic renewals of 90-day fraud alerts; and
  - $1 million identity theft insurance.
- Telephone call center with toll-free number.
- FAQs posted on DHCS Web site with referrals to resources.
- Outreach to Key Third Parties with information for impacted individuals.
- Responded to numerous media inquiries.

Investigation & Corrective Action Plan

- Causes of breach: ad hoc request with short turn-around
- Mailing vendor did thorough review, instituted strict quality control procedures and required additional staff training
- DHCS conducted thorough investigation and took immediate steps to prevent a similar incident
- DHCS also reviewed internal policies and procedures and adopted new security procedures:
  - improved controls for data releases of PHI and PI; and
  - quality assurance controls for electronic data

At Time of the Breach



At Time of the Breach

Missed Opp. #1

Check Point #1

Missed Opp. #2

Check Point #2

Missed Opp. #3

Check Point #3

Requested mailing

BWARD / MCED

Data File created

ITSD – Main Data Source for Medi-Cal

File created for HCO, Dental, HP

Date File sent to Contractor – Mailhouse Ops.

Two secure e-mails sent; 1) the actual Excel data file & 2) the password

Contractor Mailhouse Ops received the Data File

This point is designed to have validated the data file

File is approved by Contractor and sent (transferred) to Extreme Dialog

Extreme Dialog is the program which takes the data formats the letters to go to K/P

K/P System Reads Extreme File

Review samples to verify mailing (Qulity Control (QC) Process)

Mailing approved by K/P and job finished

Letters are picked up by US Post Office for mailing in this case; in other cases K/P sends to presort vendor and they deliver to the US Post Office

Contractor conducts Q/A

Contractor does QC on samples of post mailings to ensure that meet contract requitements.

Last Fridays Review w/HCO

Data File created

ITSD – Main Data Source for Medi-Cal

Additional New Check Point

File sent over to DHCS/HCOB Systems Support Unit (SSU)

Reviewed for irregularities in date file layout

DHCS/HCOB SSU post on DHCS shared drive

Location where file is posted to Contractor Info System (IS) to retrieve.

Additional New Check Point

Contractor's IS Shop retrieves data file and reviews

An additional check point process involving the Contractor's IS staff

Additional New Check Point

DHCS/HCOB staff at K/P

HCOB staff will be on-site for these mailing to conduct additional

Lessons Learned

- Importance of being prepared: DHCS' handling of the incident was enhanced by immediate identification of the core response team, involvement of staff with program expertise, and involvement of Office of Public Affairs with its expertise.

Lessons Learned (Con’t)

- Importance of immediate and precise coordination between members of the core response team: Members of the core response team made decisions and implemented DHCS’ response as an emergency incident that required 24/7 handling.

Lessons Learned (Con’t)

- Importance of outreach to stakeholders: population was particularly vulnerable

- It also made DHCS’ response more transparent and improved public perception of DHCS and its response.

DHCS Data Release Policy

- Confidential data must not be released or transmitted external to DHCS without a fully approved **Data Release Approval Form**
- Division chief, the data owner, Privacy Officer and Information Security Officer must approve the release
- Division data release coordinators track and document releases

DHCS Data Release Approval Process

ROLES & RESPONSIBILITIES

- **Program Requesting - *Division Chief or Designee***
  - Review/approve according to division policies
  - Review for minimum necessary
- **Program Requesting - *Data Release Coordinator***
  - Assign control number and route for signatures
  - Review for completeness and accuracy
  - Division single point of contact for data releases
  - Archive copy of fully signed form
- **Data Owner - *Division Chief or Designee***
  - Review/approve according to data policies/procedures
  - Review for minimum necessary

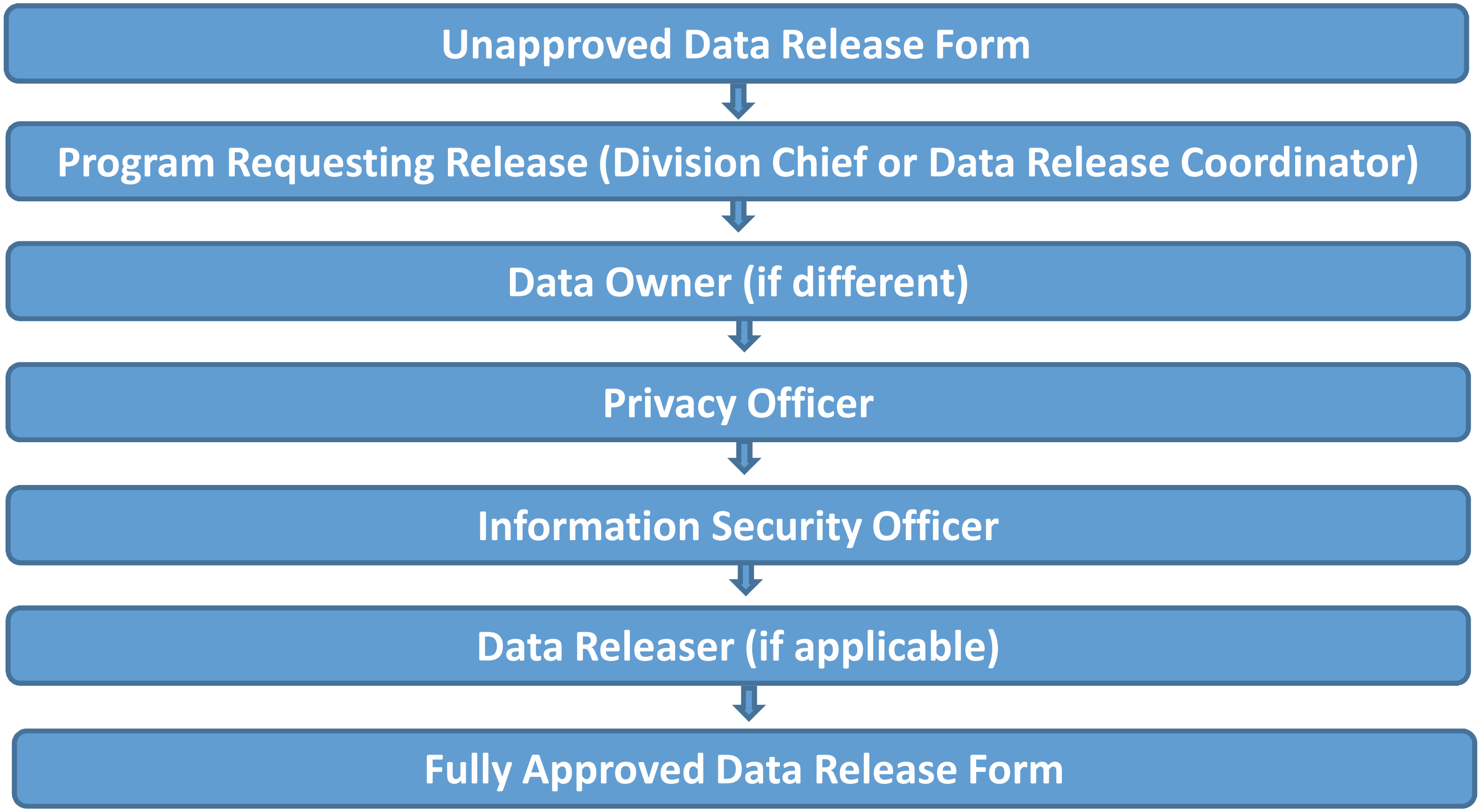
DHCS Data Release Approval Process

ROLES & RESPONSIBILITIES

- **Privacy Officer**
  - Review/approve for legality of data release
- **Information Security Officer**
  - Review/approve technical security controls
- **Data Releaser**
  - Management review/approval of release methodology
  - Ensure actual release matches data release form
  - Verify minimum necessary
  - Verify data being sent is no more than necessary
  - Transmit data securely
  - Verify accuracy of recipient address
  - Maintain chain of custody logs
  - Store copy of signed data release forms

Process Flow for All Data Release Approvals

- Flowchart describing the flow of forms and responsibilities:



Unapproved Data Release Form

Program Requesting Release (Division Chief or Data Release Coordinator)

Data Owner (if different)

Privacy Officer

Information Security Officer

Data Releaser (if applicable)

Fully Approved Data Release Form

Quality Assurance Procedures

- A form “Data Release (DR) Quality Assurance (QA) Process” is used to ensure the actual release of electronic data matches what is on the approved data release form.
- The data validation consists of:
  - Does the data contain a Social Security Number (SSN)?
    - If yes, is this a required field for this release?
  - Does the requested record length match the data file record length?
  - Do the requested record fields match the fields in the data file?
  - Does the content of the data file match the requested criteria
    - (Example County, aid code, plan, time period…)?
  - Is the file size the expected size for this request?

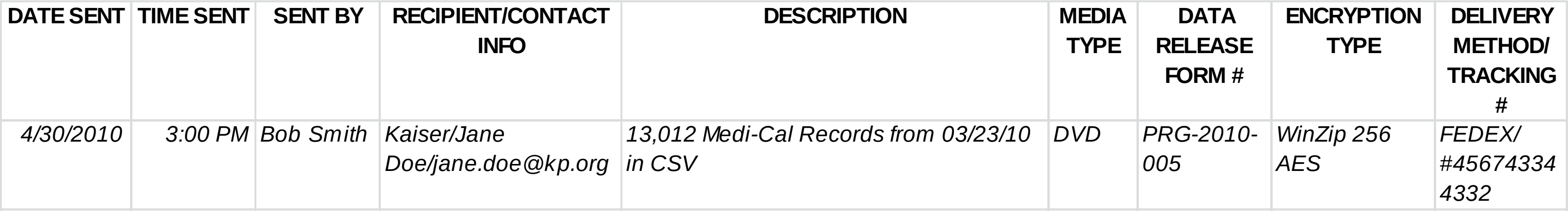
Quality Assurance Procedures

  - Does the expected row count match the control totals of the output jobs?
  - Is the date of release approved on the Data Release Form still valid?

- Two senior level ITSD reviewers, including a reviewer independent from the staff member who compiled the data and an ITSD manager, must sign this form.

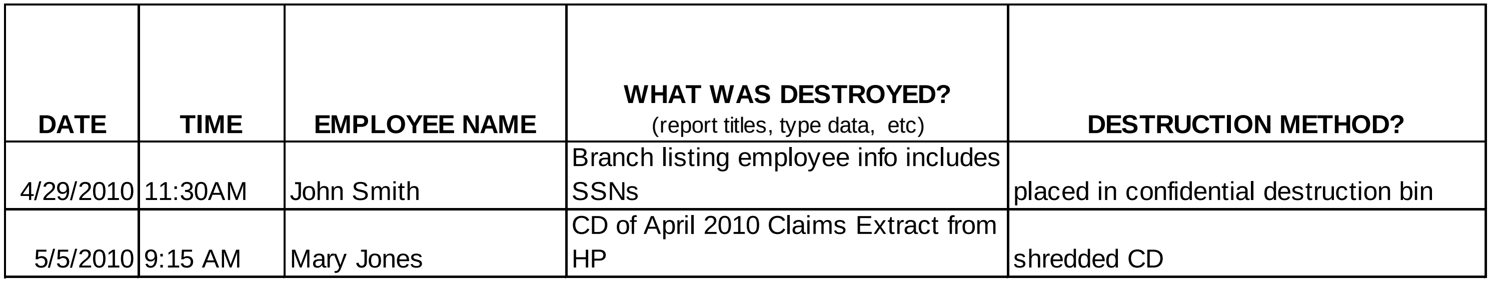
Sample Tracking Logs

- Logging individual transfers:



DATE SENT	TIME SENT	SENT BY	RECIPIENT/CONTACT INFO	DESCRIPTION	MEDIA TYPE	DATA RELEASE FORM #	ENCRYPTION TYPE	DELIVERY METHOD/ TRACKING #
4/30/2010	*3:00 PM*	*Bob Smith*	*Kaiser/Jane Doe/jane.doe@kp.org*	*13,012 Medi-Cal Records from 03/23/10 in CSV*	*DVD*	*PRG-2010-005*	*WinZip 256 AES*	*FEDEX/ #456743344332*

- Destruction of data:



DATE	TIME	EMPLOYEE NAME	WHAT WAS DESTROYED? (report titles, type data, etc)	DESTRUCTION METHOD?
4/29/2010	11:30AM	John Smith	Branch listing employee info includes SSNs	placed in confidential destruction bin
5/5/2010	9:15 AM	Mary Jones	CD of April 2010 Claims Extract from HP	shredded CD

External Research Data Requests

- Each year, researchers from across the United States request Medi-Cal data
- Medi-Cal collects and maintains one of the largest administrative data sets in the world
- Medi-Cal data contains so many observations that even infrequently occurring events are represented in large enough numbers that they can be studied
- DHCS releases electronic files with vast amounts of data (50,000, 1 million, up to 10 million records at a time) to other state departments, contractors (fiscal intermediary, health care plans), and health care oversight agencies (CMS, Bureau of Medi-Cal Fraud and Elder Abuse) and other entities

Data and Research Committee (DRC)

- The DRC was formed in the fall of 2008 to review protected data requests from external researchers.
- The DRC makes recommendations to DHCS management regarding how the department works with external researchers.
  - External researchers: Any entity (usually university staff or faculty) outside of DHCS carrying out research.
    - May include researchers in other state departments, such as CDPH.
  - This does not include the release of information for internal program evaluation or administrative purposes.
  - Application process: http://www.dhcs.ca.gov/dataandstats/data/Pages/AccessingProtectedData.aspx

Data and Research Committee (DRC)

- DRC addresses requests for all levels of data:
  - De-identified (no HIPAA identifiers)
    - *De-identified data is not restricted in its release*
  - Limited data set (may contain certain HIPAA identifiers)
- The Department is not required to release Medi-Cal data to researchers
- The Department may release such data assuming the research endeavor will result in information that is directly connected with the administration of the State plan
  - DRC determines whether a research request is of benefit to the Medi-Cal program and worth the effort to assist the researcher

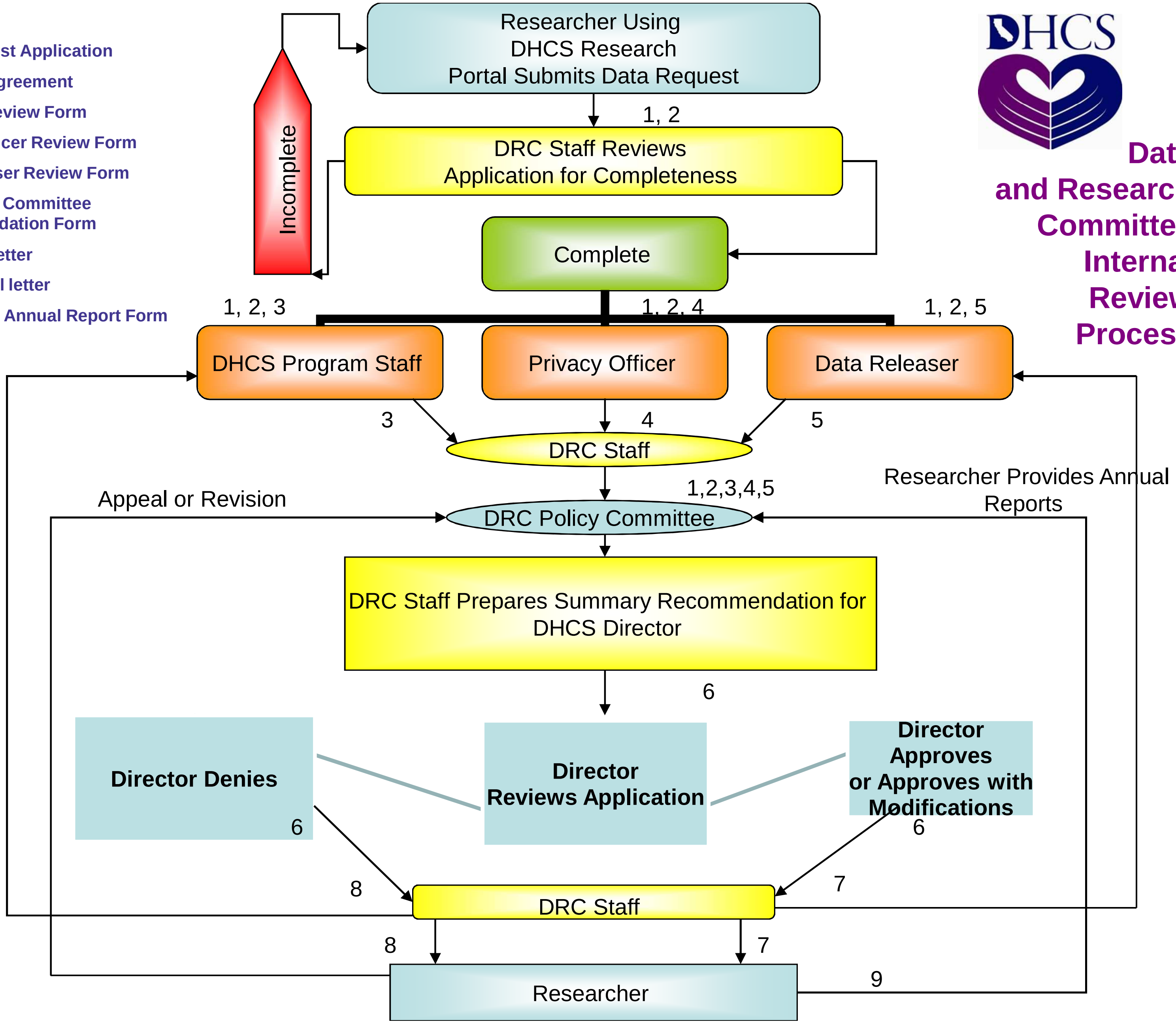
DRC Structure

- DRC members meet bimonthly and consist of a representative from each of the following entities:
  - Privacy Office/Legal Services
  - Information Technology Services (ITSD)
  - Office of Women’s Health
  - Fiscal Forecasting/Research & Analytic Studies
  - Managed Care
  - Pharmacy Benefits
  - Benefits, Waivers Analysis and Rates

Data and Research Committee Internal Review Process

FORM LEGEND

1. Data Request Application
2. Data Use Agreement
3. Program Review Form
4. Privacy Officer Review Form
5. Data Releaser Review Form
6. DRC Policy Committee Recommendation Form
7. Approval Letter
8. Disapproval letter
9. Researcher Annual Report Form



Researcher Using DHCS Research Portal Submits Data Request

1, 2

DRC Staff Reviews Application for Completeness

Incomplete

Complete

1, 2, 3

1, 2, 4

1, 2, 5

DHCS Program Staff

Privacy Officer

Data Releaser

3

4

5

DRC Staff

1,2,3,4,5

Appeal or Revision

Researcher Provides Annual Reports

DRC Policy Committee

DRC Staff Prepares Summary Recommendation for DHCS Director

6

Director Denies

6

Director Reviews Application

Director Approves or Approves with Modifications

6

8

7

DRC Staff

8

7

Researcher

9

DRC Approvals

- Since the fall of 2009, 54 research proposals have been reviewed at a total of 16 DRC meetings. Of these 54 proposals, 21 new projects and 22 renewals (a total of 43 proposals) have been officially approved.
- A link to DRC approved projects:

http://www.dhcs.ca.gov/dataandstats/data/Pages/ListofApprovedDRCProjects.aspx

- A link to some publications that have resulted from research using DHCS data:

http://www.dhcs.ca.gov/dataandstats/data/Pages/ListofPublications.aspx

External Research Data Request Example

- Dr. Singh, a Stanford University professor, used Medi-Cal paid claims data to determine that Vioxx posed a health risk.
- The Medi-Cal data was used to isolate patients that experienced a certain life threatening side effect. Eventually this resulted in a voluntary worldwide withdrawal of Vioxx by Merck.
- The Medi-Cal data set contained enough events that the researcher could study the life threatening event, developing statistically meaningful results.

Contact Information

Karen Johnson, C.P.A.

Chief Deputy Director

California Department of Health Care Services

Karen.Johnson@dhcs.ca.gov

(916) 440-7868 direct

P.O. Box 997413, MS 0000

Sacramento, CA 95899-7413