



Prescription for a More Secure Practice

Basic Security Tips from the
California Attorney General's Office



Joanne McNabb

CIPP/US, CIPP/G, CIPT

Director of Privacy Education & Policy
California Attorney General's Office



AG's Privacy Unit

- Enforces Constitutional privacy right and civil privacy statutes
- Empowers consumers with information and strategies
- Encourages businesses to adopt privacy-respectful practices
- Advises the AG on privacy matters



Data Breaches Today

12 USA TODAY
A GANNETT COMPANY

NEWS SPORTS LIFE **MONEY** TECH TRAVEL OPINION 82° CROSSWORDS YOUR TAKE

Another health care data breach

Steve Weisman, for USA TODAY 9:02 a.m. EDT July 25, 2015

f 132
t 183
in 257
4
EMAIL
MOR

(Photo: Thinkstock)

Following close on the heels of the massive data breach at health insurer Anthem, the parade of hackings at major health care providers continues with the recent announcement of a data breach at [UCLA Health System](#) affecting 4.5 million people. The hacking appears to have gone on undetected





CA Breach Notification Law

- CA Civil Code 1798.82 and 1798.29
- Applies to
 - Any person or business doing business in CA; state and local gov't agencies



CA Breach Notification Law

- Breach defined
 - Acquisition – or reasonable belief of acquisition – by an unauthorized person
- Information covered
 - Unencrypted, “computerized data”
 - Name + SSN, DL#, financial acct. #, medical info, health insurance info, or ALPR data
 - Online account credentials (user ID/email+PW or security Q&A)



CA Breach Notification Law

- Timing of notification
 - Most expedient time possible and w/out unreasonable delay
 - Delay allowed to “restore the reasonable integrity of the system” and to determine the scope
 - Delay allowed if law enforcement says would impede criminal investigation



CA Breach Notification Law

- Method of notification
 1. Written
 2. Electronic – only per E-SIGN Act
 3. Substitute – only if $> \$250,000$ or $> 500,000$ people or insufficient contact info
 - Web site, AND
 - Email, if known, AND
 - Statewide media
 4. Online – only for breaches of online account credentials



Notice Format & Content

- Name & contact info of notifying entity
- Types of personal info involved
- Date of breach and general description (if known at time)
- In breach of SSN or DL#, contact info for CRAs and offer of ID theft prevention service (1 yr.)

Acme Corporation

January 30, 2015

Sample A. Sample
Apt ABC
123 Any St
Anytown, US 12345-6789

Notice of Data Breach

What Happened

On June 23, 2014, an Acme Corporation laptop computer containing personal information was stolen from an employee's home. The employee reported the theft to law enforcement and to Acme. A law enforcement investigation is underway.

What Information Was Involved

The information on the laptop included your Social Security number. Other personal information that may have been on the laptop includes your name; drug test results; bank account number; date of birth and driver's license number.

What We Are Doing

We deeply apologize for this incident and have taken actions to prevent any re-occurrence. We have hired experts to help us determine whether the laptop actually contained personal information at the time of the theft. We are also reviewing our internal policies and procedures related to protecting our employees' information.

As an extra protection for you, we are offering a complimentary one-year membership in Experian's® ProtectMyID® Elite product. See the attached sheet for details and how to enroll.

What You Can Do

Because your Social Security number was involved, you may want to place a fraud alert on your credit files. This alerts creditors to take additional steps to verify identity before granting new credit in your name. Placing a fraud alert is free. See instructions on the attached sheet.

We recommend that you regularly review any statements that you receive from your bank or credit card company. If you see items on the statement that you do not recognize, immediately contact the bank or credit card company.

For More Information

If you have questions about this incident or the contents of this notice, please call 1-877-218-2930, Monday through Friday, 10:00 AM to 7:00 PM EST. Please use reference number 7386061314 when calling.



CA Breach Law - Penalties

- Enforced through unfair competition law, Bus. & Prof. Code § 17200 and following.
- Penalties include injunctive relief, civil fines of up to \$2,500 per violation



CA Breaches Reported to AG

State of California Department of Justice
Office of the Attorney General

Kamala D. Harris ~ Attorney General

Home About the AG In the News Careers Services & Information Programs A-Z Contact Us

Cybersafety > eCrime > Search Data Breaches

SEARCH DATA SECURITY BREACHES

California law requires a business or state agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. (You can read the law here: California Civil Code s. 1798.29(a) for state agencies and California Civ. Code s. 1798.82(a) for businesses).

The law also requires that a sample copy of a breach notice sent to more than 500 California residents must be provided to the California Attorney General. Below is a list of those sample breach notices. (Note that in some cases the organization that sent the notice is not the one that experienced the breach. For example, a bank may notify of a credit card number breach that occurred not at the bank, but at a merchant.)

You can search by the name of the organization that sent the notice, or simply scroll through the list. To read a notice, click on the name of the organization in the list. Then click on the link titled "Sample Notification."

Organization Name:

Date of Breach Range: From To
E.g., 2015-08-13 E.g., 2015-08-13

Organization Name	Date(s) of Breach	Reported Date
Internet Corporation for Assigned Names and Numbers - ICANN	07/31/2015	08/12/2015
Nationstar Mortgage LLC	07/27/2015	08/12/2015
SterlingBackcheck	05/29/2015	08/07/2015
WP Technology Inc. d/b/a Wattpad	05/26/2015	08/06/2015
Mama Mio US, Inc.	04/28/2015	08/04/2015
orientino dyoco, M.D.	08/03/2015	08/03/2015
North East Medical Services	07/11/2015	07/31/2015
Orange County Employees Association	06/05/2015	07/31/2015
East Bay Perinatal Medical Associates	06/01/2015	07/29/2015
Golden 1 Credit Union	04/07/2015, 08/17/2015	07/27/2015
American Express Travel Related Services Company, Inc and /or its Affiliates ("AXP")	02/01/2015	07/27/2015

Data Security Breach (SB24)

- Data Security Breach Reporting
- Submit Data Security Breach
- Search Data Security Breaches

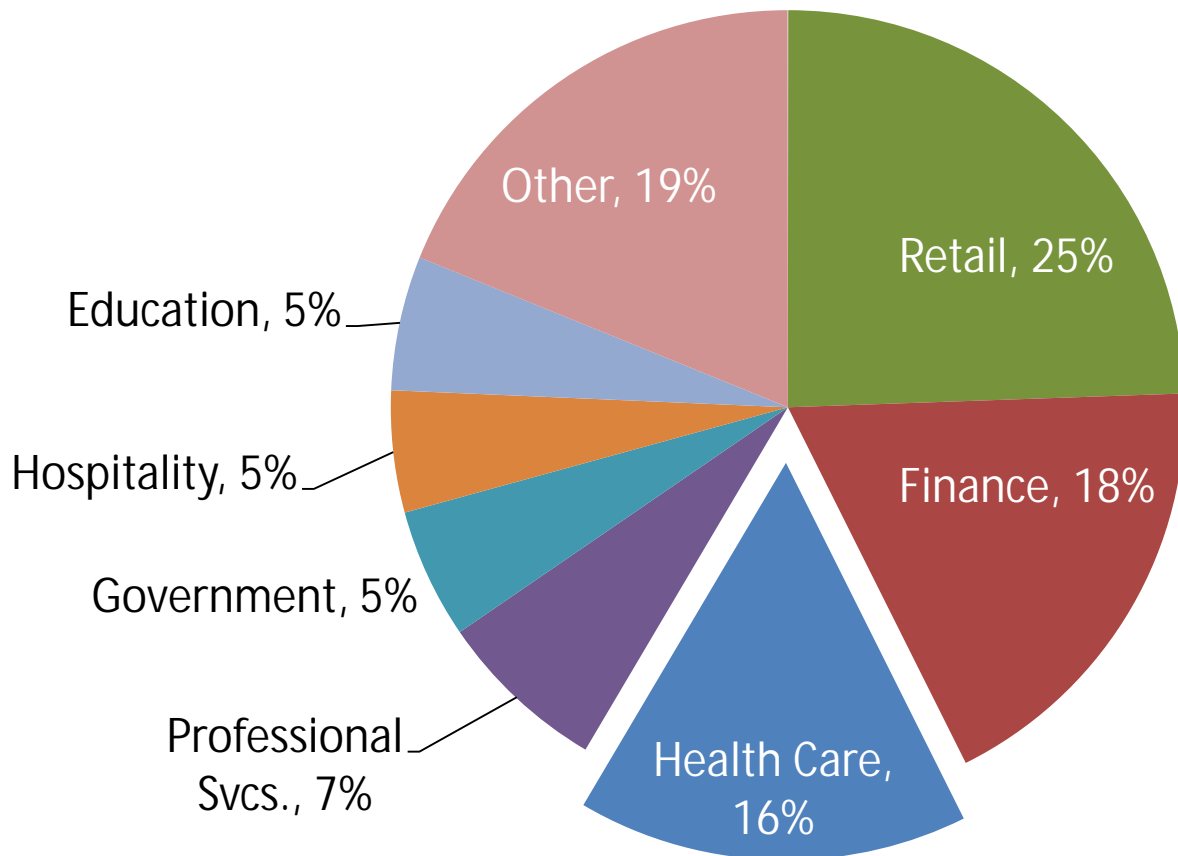
Related Information

- 2012 Data Breach Report, pdf
- 2014 Data Breach Report, pdf
- Breach Help: Tips For Consumers
- Cybersafety
- Data Breach Statistics, pdf
- eCrime
- Identity Theft
- Privacy

Breaches affecting > 500 Californians must be reported to AG.



CA Data Breaches by Industry

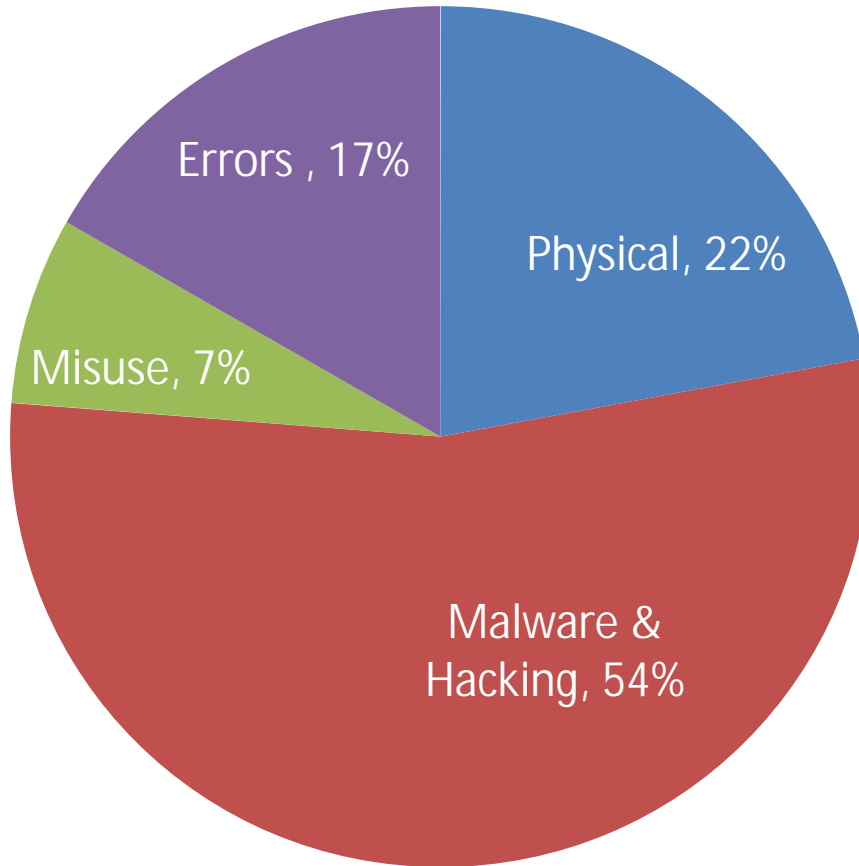


2012-2015

- 657 breaches
- >500 CA residents



CA Data Breaches by Type

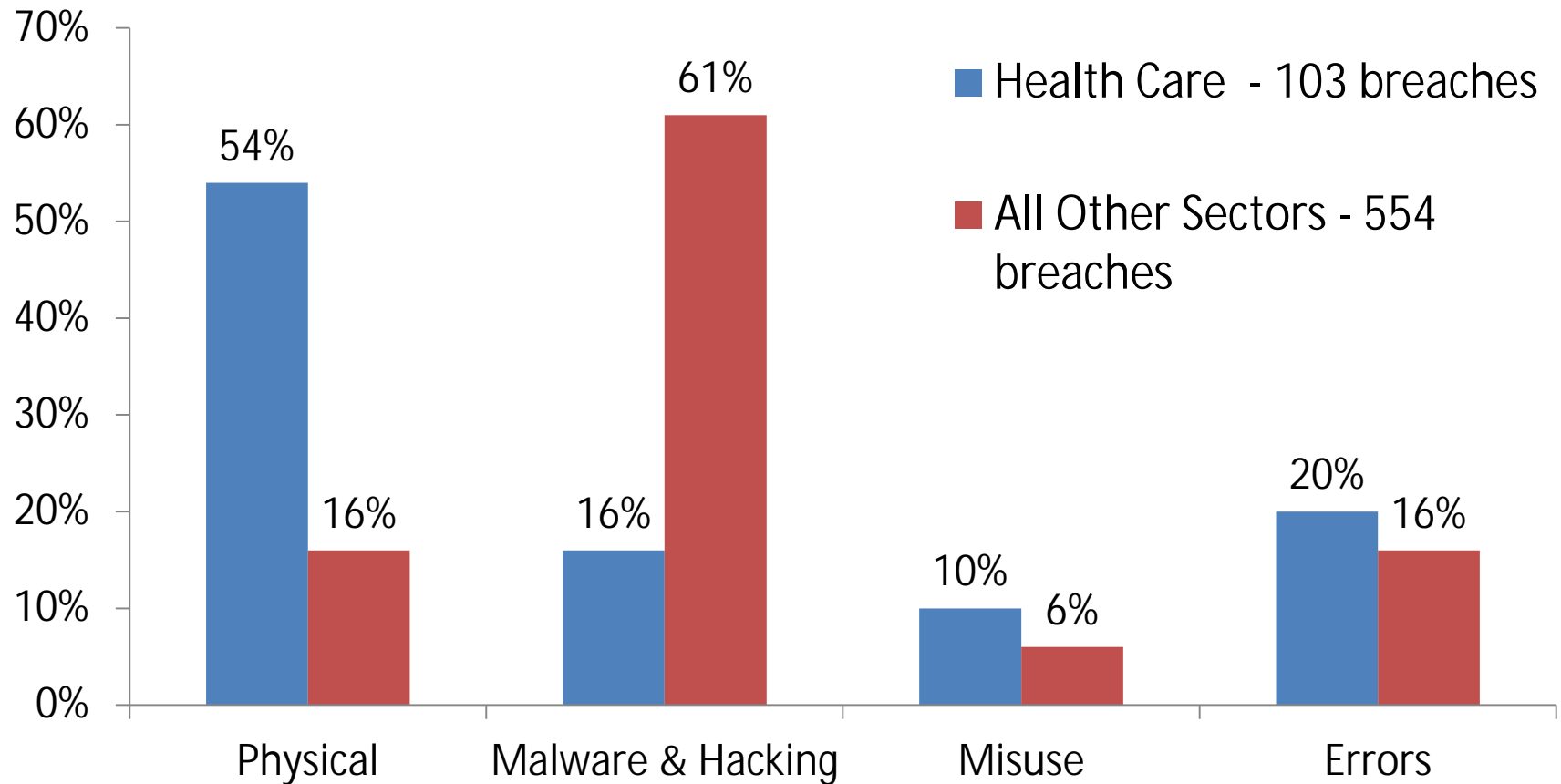


2012-2015

- 657 breaches
- >500 CA residents

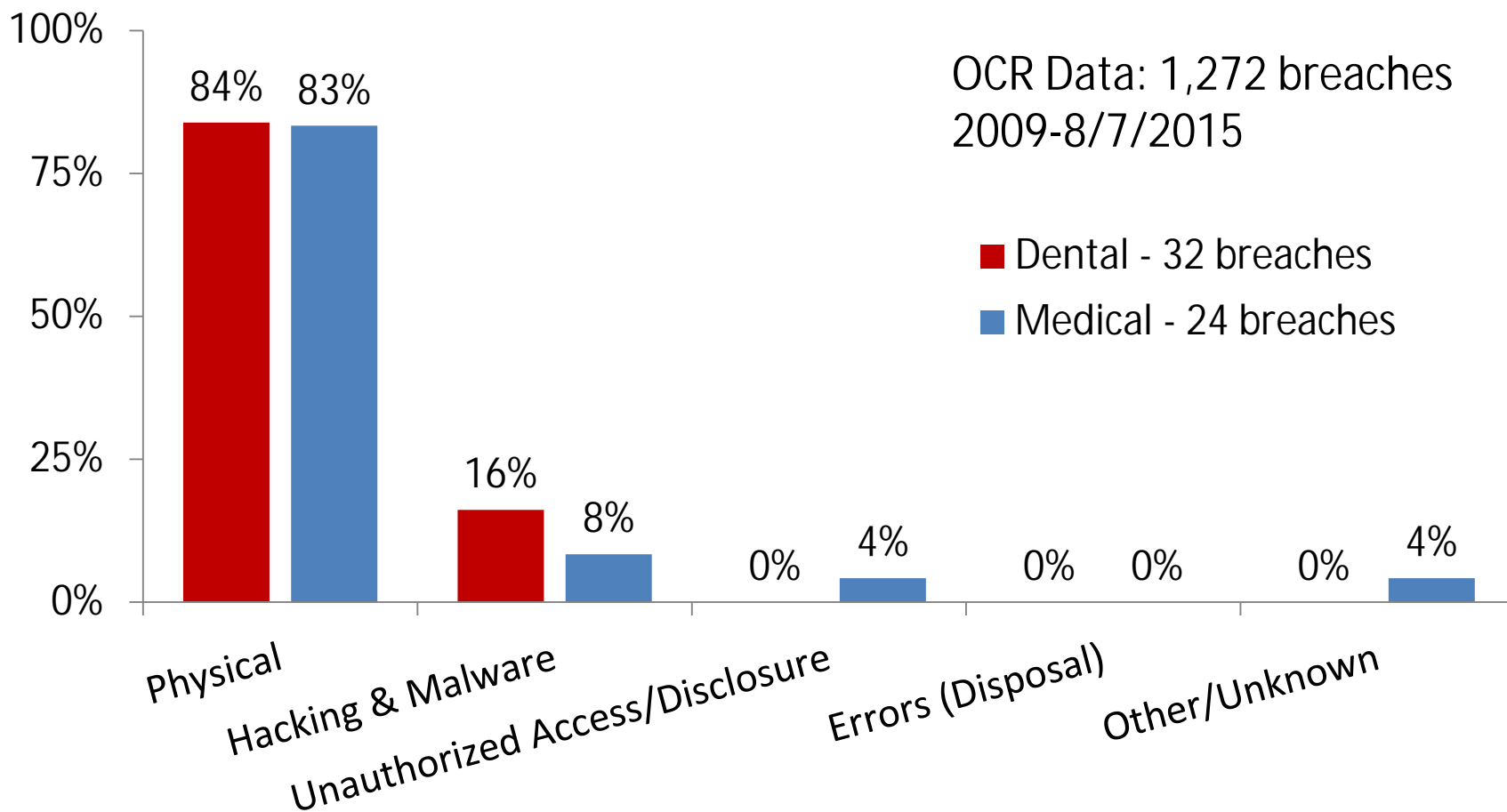


CA Health Care Breaches





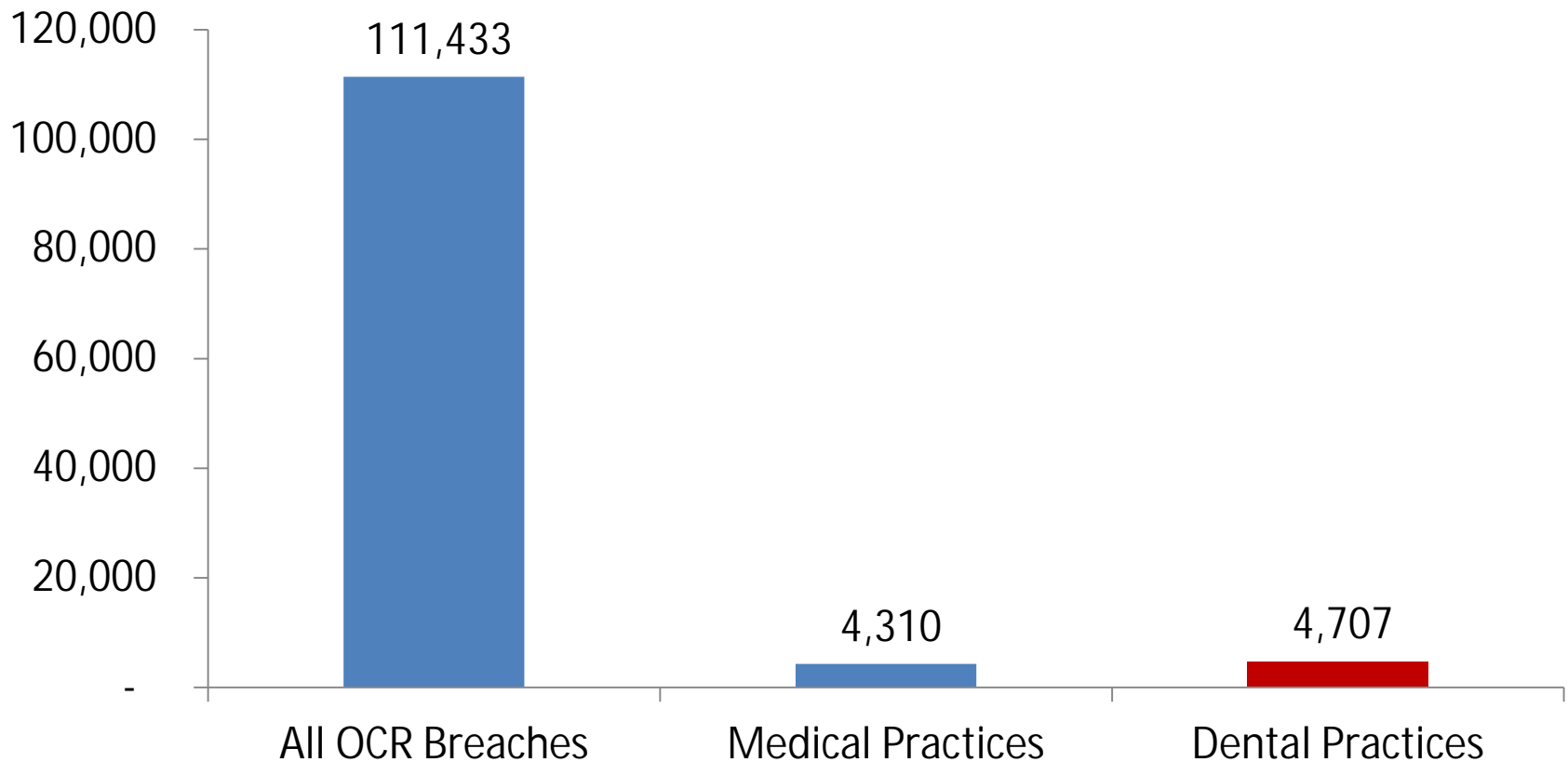
Breaches in Medical & Dental Practices





Medical & Dental Practice Breaches – Number Affected

Average Number Affected per Breach





Cost of a Dental Data Breach

- Average dental practice breach 4,700 records (OCR data)
- Cost estimated at from **\$100,000 to over \$1 million**
 - Direct costs (mailing, forensics, mitigation product)
 - Indirect costs (in-house investigation and communication, client loss)



Preventable Dental Breaches

- USB drive with unencrypted patient data lost in mail
- Laptop with unencrypted patient data stolen from car/home/office
- Desktop computer with unencrypted patient data stolen from office



Filling the Cavities in Your Practice

Lock

Encrypt



www.privacy.ca.gov