

International Dosimetry Symposium
Portland, ME June 5, 2007

Implications of the “Privacy Movement” on a Corporate Radiation Safety Program

S. Elizabeth Kay, T.L. Mays

Lilly Research Laboratories, Health Safety and Environment
Eli Lilly and Company, Indianapolis, IN

The Lilly logo is a stylized, cursive script of the word "Lilly" in white, positioned in the bottom right corner of the slide.

Answers That Matter.

Introduction

So what do a Shoe Salesman and a Health Physicist
have in common?



HPs and Sensitive Personal Information

- Security/Background Checks
- Positive Identification
- Dose Tracking using SSN



Regulatory Review: How did we get here?

Regulatory Guide 8.7: *Instructions for Recording and Reporting Occupational Radiation Dose Data*

“The use of licensee-generated identification numbers should be avoided whenever possible.”

REIRS/REMS Reporting require “unique identifier”

CRCPD Regulations Template

Regulatory Review (Continued)

Excerpt from NRC Form 5 Privacy Act Statement

4. **WHETHER DISCLOSURE IS MANDATORY OR VOLUNTARY AND EFFECT ON INDIVIDUAL OF NOT PROVIDING INFORMATION:** It is voluntary that you furnish the requested information, including social security number (identification number); however, the licensee must complete NRC Form 5 on each individual for whom personnel monitoring is required under 10 CFR 20.2106. Failure to do so may subject the licensee to enforcement action in accordance with 10 CFR 20.2401. The social security number (identification number) is used to assure that NRC has an accurate identifier not subject to the coincidence of similar names or birth dates among the large number of persons on who data is maintained.

Bottom Line: NRC does not require SSN

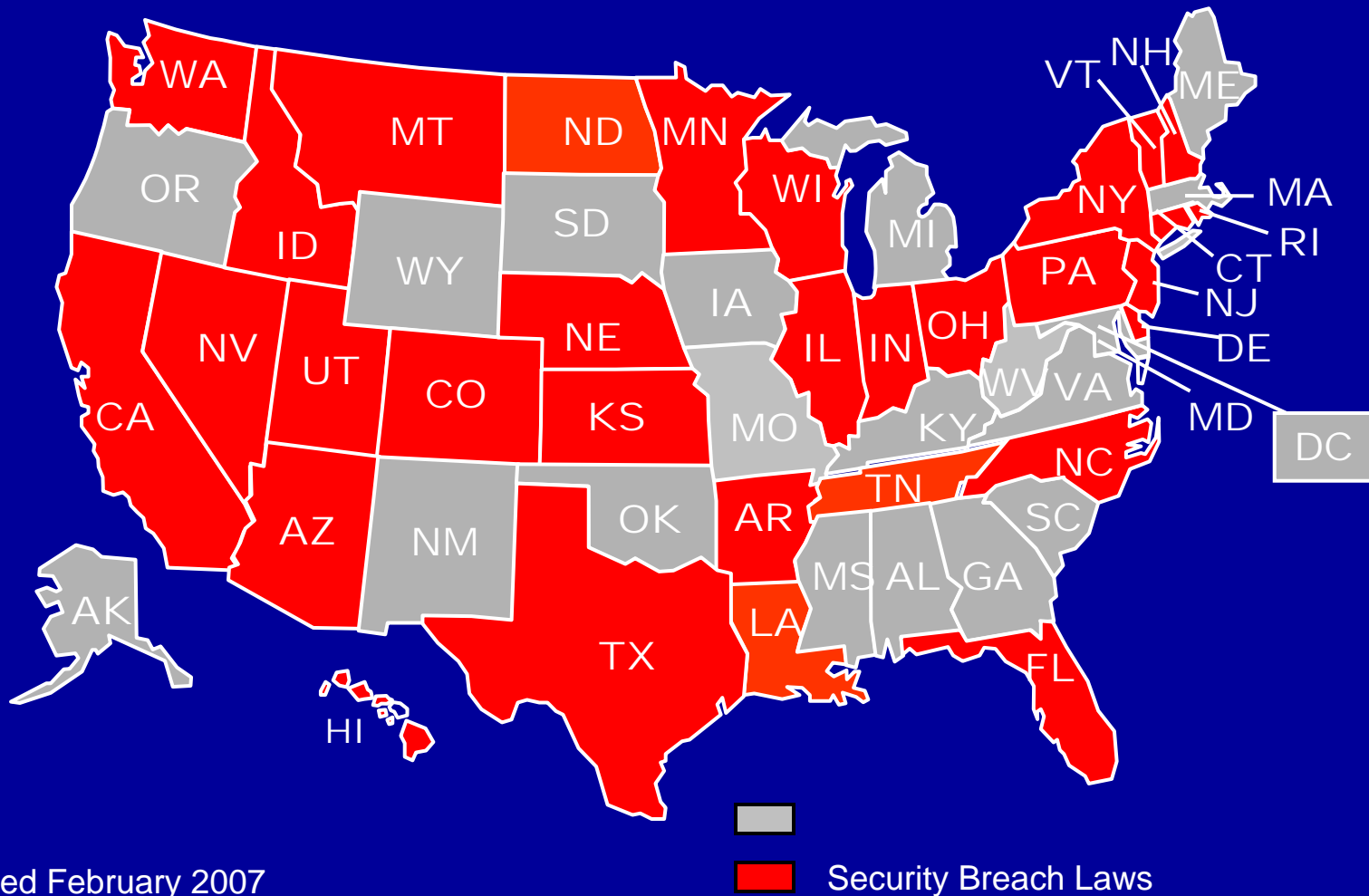
State Privacy Laws

Breach Notification Laws (approx. 30 states, as early as 2003, but many effective in 2006 and 2007)

- Loss/theft of Name + SSN requires notification to individual
- Individual Notification or via Media



States with Security Breach Laws



Last Updated February 2007

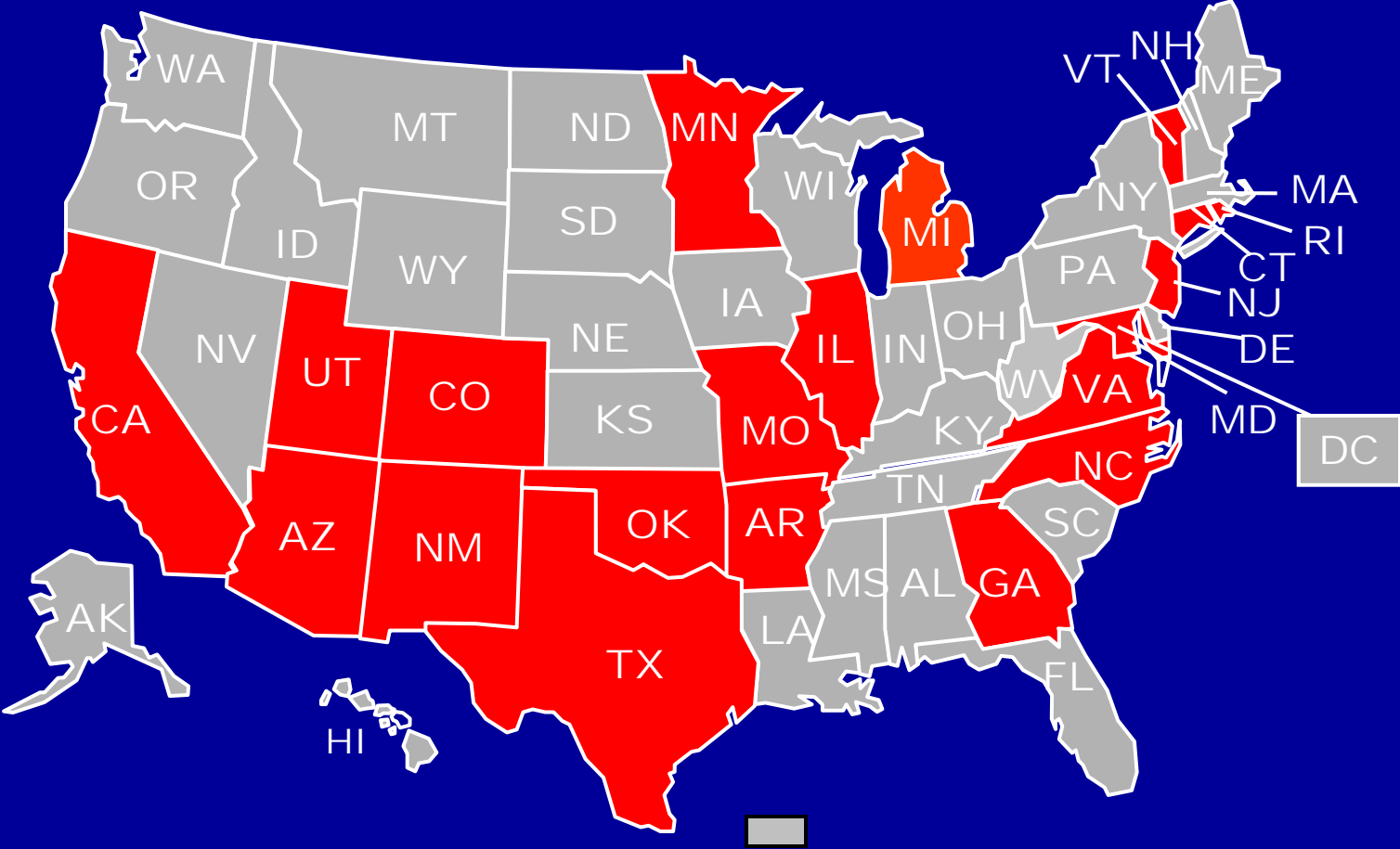
State Privacy Laws

SSN Restriction (Approx 20 states, starting as early as 2002, but many effective in 2006, 2007)

- Posting, requesting SSN may be illegal
- SSN Policies may be required



States with SSN Restrictions



Last Updated February 2007

■ SSN Restrictions

Federal Privacy Law

Currently No Federal Law BUT...

Personal Data Privacy and Security Act of 2007

S.495: P. Leahy (D-Vt) B. Sanders (I-Vt)

- Data Privacy and Security Requirements
- Security Breach Notification

Common Practice? (an informal poll)

- Still common to get question/pushback when asking for SSN
- Institutional pressure to defend/discontinue collection of SSN is on the rise
- Some RSOs have chosen an alternative unique identifier

Risk Assessment : Dose Tracking **without SSN**

Regulatory/Health and Safety

Potential for overexposure in cases where a Radiation worker receives dose under multiple licenses

Social/Scientific

Loss of Epidemiological Evidence (REMS/REIRS)

Legal

Weak unique identifier could result in dose records ruled as “hearsay” and inadmissible as evidence resulting in multi-million dollar judgment (Health Phys. 81(6):683-690; 2001)



Risk Assessment : Dose Tracking with SSN



Legal

Compliance with multiple SSN and breach notification laws

Social/Criminal

Identity theft

Financial

Impact on consumer trust and brand

Licensee Actions to Minimize Risk

- Use an alternative unique identifier or;
- IT Security Controls
 - Access control
 - Use of truncated SSNs when possible
 - Eliminate sensitive information from dose reports

Third Party Considerations

- Regulatory Agencies: (NRC) RIS-2007-04
“Personally Identifiable Information Submitted to the U.S. Nuclear Regulatory Commission”
- Dosimetry Providers (leverage NVLAP accreditation?)
- Due Diligence
 - Privacy Policy?
 - Audits?
 - Previous History of Breach?
 - IT system security?

Conclusion

Assess risk balance as the Privacy movement continues to evolve...

