# Government Access to Personal Medical Information Task Force

C.R.S § 24-72-603 (as amended by HB 14-1323)

KATE KIEFERT, TASK FORCE CO-CHAIR

RONNE HINES, TASK FORCE CO-CHAIR

State of COLORADO

## Agenda

- HB 14-1323 Key Objectives
- Task Force Process
- Key Findings
  - Federal and State Laws Protecting Health Information
  - Government Access to Health Information
  - Policies & Procedures for Ensuring Safe Access & Mitigating Risk
  - Concluding Summary & Recommendations for Next Steps
- Questions

# HB 14-1323 Key Objectives

House Bill 14-1323 established the Government Access to Personal Medical Information Task Force ("Task Force") to review and analyze government access to personal medical information

In accordance with HB 14-1323, the Task Force's key objectives were to:

- Conduct an environmental scan of the existing laws governing access to health information
- Obtain information on how state agencies implement policies and procedures to ensure safety and privacy of health information when it is properly collected
- Ensure agencies have policies in place to mitigate the risk of privacy or security breaches and respond to breaches if they occur
- Develop recommendations to ensure state and local governments are able to continue fulfilling their commitments to protect Colorado consumers and their health information

# Task Force Process

Summer of 2014 – The Task Force

- Reviewed the legislation, questions, and topics outlined
- Determined one-on-one interviews should be conducted with each governmental and nongovernmental entity participating in the Task Force (see list below)
- Established a set of key questions to address the topics identified in legislation*

| State Agencies and Departments | Nongovernmental Entities |
|---|---|
| • Colorado Department of Corrections<br>• Colorado Department of Health Care Policy and Financing<br>• Colorado Department of Higher Education<br>• Colorado Department of Human Services<br>• Colorado Department of Labor and Employment<br>• Colorado Department of Law<br>• Colorado Department of Personnel and Administration<br>• Colorado Department of Public Health and Environment<br>• Colorado Department of Public Safety<br>• Colorado Department of Regulatory Agencies<br>• Colorado Department of Revenue<br>• Colorado State Auditor's Office | • Colorado Association of Health Plans<br>• Colorado Counties Incorporated/County Technical Services, Inc.<br>• Colorado Municipal League<br>• Colorado Psychiatric Society<br>• Connect for Health Colorado<br>• COPIC Insurance<br>• Mental Health America of Colorado<br>• University of Colorado |

*See Appendix B of the Task Force report

# Key Findings

- Privacy of personal information has long been an important issue
- Health information is a particularly sensitive subset of information
- Benefits of health information when accessed and used appropriately
  - Can save or improve lives
  - Ensure effective use of resources
  - Enable government agencies to fulfill their statutory obligations (examples below)

| Government Agencies | Healthcare Settings |
|---|---|
| • Monitor communitywide trends<br>• Develop adequate responses to outbreaks of contagious disease or environmental hazards | • Improve quality and convenience of patient care<br>• Enhance accuracy of diagnoses and health outcomes<br>• Promote care coordination<br>• Ensure patient safety<br>• Result in greater efficiency and cost savings |

- Balancing the need to protect health information with the need for effective healthcare and government services has resulted in ample state and federal law

# Federal and State Laws Protecting Health Information

**Health Insurance Portability Accountability Act (HIPAA)**

- Protects the privacy of individually identifiable health information
- Sets national standards for electronic medical records
- Enforced by U.S. Department of Health and Human Service's Office of Civil Rights
- Serves as a critical privacy floor and regulatory umbrella for most health information, whether accessed by a government agency, nongovernmental entity, or private business
- Agencies that qualify as covered entities under HIPAA must have a designated privacy official responsible for overseeing HIPAA compliance
  - Ensuring privacy guidelines are followed
  - Providing education to employees
  - Adhering to requirements of regular audits

**State laws***

- State laws that conflict with HIPAA are unenforceable unless they offer more stringent protections for personal privacy

**Patient Consent**

- Requiring patient consent for use of identifiable health information helps to ensure proper balance between protecting sensitive information and allowing that information to be used at its highest potential
- Giving patients consent power alleviates concerns about using health information for beneficial purposes because it affords the individual control over their own data

*See Task Force Report Appendix D

# Key Findings

- Three primary reasons law authorizes access to health information by government agencies:
  - To determine or verify **eligibility** for public services and programs;
  - To contribute to community-level, **de-identified data surveillance and analysis**;
  - To enable agencies to **enforce regulations** that protect public health and safety.
- As an employer, state and local government agencies have restricted access to some health information related to their employees

# Public Program Eligibility

- The following state agencies rely on medical information to determine eligibility for publicly-funded benefits:
  - Colorado Department of Health Care Policy and Financing
  - Colorado Department of Public Health and Environment
  - Colorado Department of Human Services

**Health Information Use Example: HCPF**
Under federal Medicaid laws, administered in Colorado by the Department of Health Care Policy and Financing (HCPF), HCPF is required to report information regarding Medicaid care in the state. HCPF collects health information to ensure eligibility for some Medicaid eligibility categories. For example, the Medicaid Elderly, Blind, or Disabled Waiver Program and the Breast and Cervical Cancer Program both require health information to determine eligibility because eligibility is based on a medical condition or functional impairment caused by a medical condition.

In addition, HCPF collects health information to fulfill its reporting obligation and to conduct analysis that is used to improve health outcomes and payments for services. Through HCPF's Accountable Care Collaborative (ACC), information on medical services is shared with Regional Care Collaborative Organizations (RCCOs) and medical providers – in compliance with HIPAA and federal Medicaid law – to help determine best practices for care and treatment and to reduce unnecessary utilization of health services and lower costs of care.

# Data Surveillance & Analysis

- Several state agencies have statutory authority to use health information to run program analysis, research and report out to the public on the findings
- All information used for analysis is aggregated and de-identified before reporting to the public or shared with other agencies
- Databases storing health information are secure and audited by state or federal agencies to ensure privacy and security controls

**Health Information Use Examples: CDPHE**
Through the Colorado Central Cancer Registry, CDPHE is able to track how frequently and at what stage cancer is diagnosed, how often it leads to death or survival, and what populations are most impacted. This information – after it is de-identified – can be used to inform policy decisions and direct resources to communities and individuals in need.

When exposure to mercury is reported to the Blood Lead Screening and Mercury-Screening Registry, local county health departments or CDPHE employees follow-up to understand the severity of the levels of mercury and to determine if there is potential for additional exposure. All follow-ups are limited to a small number highly trained staff who ensure the individual's privacy is maintained. In addition, individuals registered with most monitoring and follow-up programs are able to refuse services. Any reports made using this data is aggregated and does not include health information that identifies the impacted individual.

# Regulatory Law Enforcement

- Access to health information may be necessary to enforce laws and regulations enacted for the purpose of promoting public health and safety. Examples of appropriate reasons to access health information:
  - Investigating complaints against licensed professionals
  - Appealing denials of insurance coverage for medical procedures
  - Prosecuting criminals
  - Ensuring proper tax collection
- Department of Regulatory Authority Divisions that may use and access health information
  - Division of Professions and Occupations (DPO)
  - Civil Rights Division
  - Division of Insurance (DOI)

## Government Employees

**Programs requiring health information to determine eligibility for state and local government employees**

- The Americans with Disabilities Act of 1990 (ADA)
- The Family and Medical Leave Act of 1993 (FMLA)
- The Colorado Workers Compensation Act of 1915 each require
- Each state agency's human resource's office has appropriate security controls in place, including but not limited to:
  - A designated individual who is trained to manage this information properly and securely
  - An employee seeking benefits initiates the application process and provides information to their designated human resources officer or authorizes their medical professional to share the information (as required by HIPAA)
  - Only information relevant to the requested benefits is required to be submitted, and these records are kept separate from the main human resources file on the individual

## Policies and Procedures for Ensuring Safe Access and Mitigating Risk

- Access to health information is vital to day-to-day operations of many state agencies
- Information is only used to fulfill statutory and regulatory obligations
- Under no circumstances does any agency have the ability to access health information for any purpose other than that which is authorized by regulations and statute, either state or federal
- Privacy and Security Best Practices
  - Requiring access to health information only be given to a limited set of highly-trained employees who require the information to complete a task
  - Requiring training upon hiring as well as annual training on HIPAA compliance and medical privacy
  - Encrypting all emails and files with health information and using secure servers to store and access information

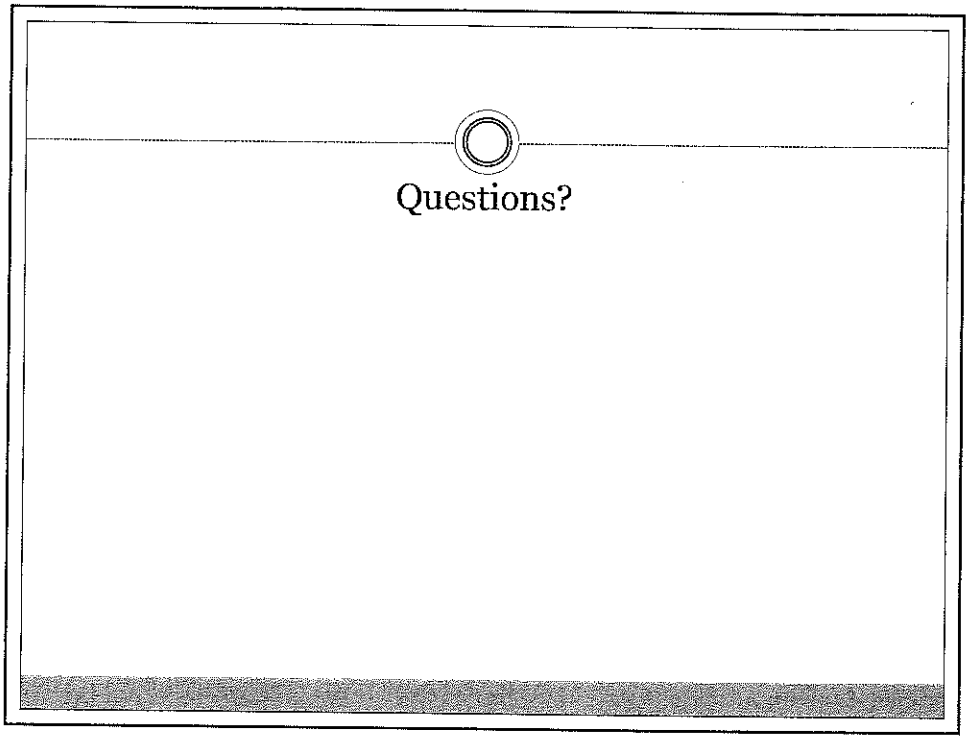
## Security of Digital Health Information & Responding to Breach

- Pursuant to HIPAA's Security Rule regulating the technical standards health information for storage and digital access, the Office of Information Technology supports information technology services for most state agencies
  - OIT is responsible for technical and physical controls, as well as internal audits of those systems
- Agencies with systems not maintained by OIT, such as HCPF, have federally-required safeguards in place to secure electronic health information
- Colorado law requires any governmental entity that has had a breach of security to notify the public through multiple means, including telephone, email, postal mail, public notice, and statewide media

## Concluding Summary and Recommendations for Next Steps

The 14-1323 Government Access to Personal Medical Information Task Force Recommendations

- Continue to ensure the security and privacy of Coloradans' health information
- Consider additional regulations limiting access could inhibit or prevent an agency's ability to fulfill its legal duties, encumber day-to-day operations, or increase costs for Colorado taxpayers
- Continue to abide by stringent procedures, and noted that within state and local government agencies, privacy guidelines are strict, well-known, and are respected by employees.
- Target any future legislative initiatives primarily at increasing public awareness and education around how their health information is used by state and local government agencies
- Inform the public about the uses of health information improves public trust
- If statutory changes are considered regarding state and local government access to personal medical information, the Task Force's primary recommendation is for the General Assembly to weigh several factors, including:
  - Whether similar existing laws are in place
  - The extent to which the proposal creates additional administrative burden and expense
  - How the public should be educated around the proposal


Questions?