Final Report of the

GOVERNMENT ACCESS TO PERSONAL MEDICAL INFORMATION TASK FORCE

November 2014

STATE OF COLORADO

John W. Hickenlooper
Governor

November 3, 2014

The Honorable Dianne Primavera
Chair, House Public Health Care &
Human Services Committee
Colorado General Assembly

The Honorable Irene Aguilar
Chair, Senate Health &
Human Services Committee
Colorado General Assembly

The Honorable Dave Young
Vice Chair, House Public Health Care &
Human Services Committee
Colorado General Assembly

The Honorable Linda Newell
Vice Chair, Senate Health &
Human Services Committee
Colorado General Assembly

Dear Legislative Colleagues:

On behalf of the Government Access to Personal Medical Information Task Force ("Task Force"), we are grateful for the opportunity to provide our analysis, findings, and recommendations regarding government access to personal medical information, as required by House Bill 14-1323 (C.R.S. §§ 24-72-603).

The attached final report reflects the efforts of the Task Force to review when, how, and why government entities access personal medical information, as well as these entities' compliance with established health information privacy laws. We are pleased to report that overall, government entities consistently employ measures to safely access and use this sensitive information, as authorized by law. A complete list of Task Force participants can be found in Appendix A.

The Task Force would like to afford special recognition to Kayla Miller and Amy Ellis, interns with the Governor's Office of Policy, Research & Legislative Affairs, for their considerable investment in time and dedication to this project.

Kind Regards,

Kate Kiefert
Co-Chair

Ronne Hines
Co-Chair

TABLE OF CONTENTS

EXECUTIVE SUMMARY

House Bill 14-1323 established the Government Access to Personal Medical Information Task Force ("Task Force"), which required appointed and invited representatives of Colorado state government, quasi-governmental entities, and statewide organizations representing county and municipal governments, healthcare providers, consumer advocacy groups, and others to review and analyze government access to personal medical information prior to November 1, 2014.[1]

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[2];
- 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; and
- Develop recommendations to ensure state and local governments are able to continue fulfilling their commitments to protect Colorado consumers and their health information.

The legislation established a set of topics to be addressed by the Task Force, which broadly covers why, how, and under what circumstances government agencies access, use, and distribute health information. In addition, Section 1 of HB 14-1323 explicitly amends Section 24-72-602, C.R.S. to address the access of personal medical information by the Colorado Department of Revenue. Appendix E-26 contains information on DOR's utilization of personal medical information and how it complies with the statutory requirements of HB14-1323 and HIPAA.

Because health information is collected and stored in a variety of ways for many uses, the Task Force's scope was quite broad.[3] In the summer of 2014, the task force reviewed the legislation, determined one-on-one interviews should be conducted with each governmental and non-governmental entity participating in the Task Force, and established a set of key questions each entity should answer. These questions are attached as Appendix B.

---

[1] House Bill 14-1323, "Concerning Restrictions on the Ability of a Government Entity to Access an Individual's Personal Medial Information," codified in pertinent part at C.R.S. § 24-72-603. Available at: http://www.leg.state.co.us/clics/clics2014a/csl.nsf/fsbillcont2/0E5F22E151FB1B9987257C3000070918/$FILE/1323_enr.pdf.

[2] House Bill 14-1323 defines "personal medical information or medical record" as "an individual's medical information or medical record...that identifies the individual; or...with respect to which there is a reasonable basis to believe the information can be used to identify the individual." While this is a strong working definition, it differs from other statutory and regulatory authorities, such as HIPAA, which references similar information as "protected health information." For the purposes of this report, to avoid confusion with the technical terms "personal medical information" or "protected health information," we will simply reference "health information."

[3] Aside from use in medical settings, health information is necessary to process insurance claims, administer applications for worker's compensation, inspect workplace safety violations, and aid law enforcement investigations. Behavioral health information presents unique challenges, in part because it benefits from heightened protections, and is outside the scope of this report.

Interviews were conducted with Task Force members of the following entities in September and October 2014:

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

Entity-specific summaries of how health information is accessed, used, and protected can be found in Appendix C.

This report provides an overview of Colorado and federal law governing access to personal medical information, discusses key findings from Task Force interviews, and discusses potential next steps to ensure the privacy and safety of Colorado consumers.

KEY FINDINGS

Privacy of personal information has long been an important issue and has steadily gained significance in light of technological advances that create new opportunities for system vulnerabilities. Health information that expressly identifies an individual or provides sufficient information to reasonably identify an individual is a particularly sensitive subset of personal information because it can contain some of the most intimate details about a person's life.

When accessed and used appropriately, health information has great potential to save or improve lives, ensure effective use of resources, and enable government agencies to fulfill their statutory obligations. For example, government agencies can use this information to monitor community-wide trends and develop adequate responses to outbreaks of contagious disease or environmental hazards. In the healthcare context, allowing access to health information by certain individuals and entities can improve quality and convenience of patient care, enhance accuracy of diagnoses and health outcomes, promote care coordination, ensure patient safety, and result in greater efficiency and cost savings.

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. Further, by ensuring that patients have a say in how their information will be used, their personal autonomy and dignity is retained. In light of the importance of patient consent, this topic is granted explicit recognition in the law.

Government Access to Health Information

Balancing the need to protect health information with the need for effective healthcare and government services has resulted in ample state and federal law. Generally, federal and state regulations protecting patient privacy have been in place for many years, and agencies have business and audit processes in place to support both appropriate access to and protection of medical records. Agencies that access and use health information have specific authorization under federal and/or state statutes or regulations.

The three primary reasons law authorizes access to health information by government agencies are: to determine or verify eligibility for public services and programs; to contribute to community-level, de-identified data surveillance and analysis; and to enable agencies to enforce regulations that protect public health and safety. In addition, as with all employers, state and local government agencies have restricted access to some health information related to their employees.

The Task Force collected citations of state and federal regulations and obligations that allow agencies to access health information; many of these are summarized in Appendix D or summarized by agency in Appendix E. As part of the Task Force's interview process, the interviewer also confirmed that no changes to policy or procedure were made regarding access to personal medical information as a result of HB 14-1323 or before interviews were conducted. The section below provides an overview of key laws and policies that impact privacy of health information, how those laws and policies are used across government agencies, and how agencies ensure compliance and enforcement of the law.

A. Health Insurance Portability Accountability Act & Privacy of Health Information

Title II of the Health Insurance Portability Accountability Act of 1996 (HIPAA), "protects the privacy of individually identifiable health information" and sets national standards for electronic medical records.[4] It is enforced by the U.S. Department of Health and Human Service's Office of Civil Rights.[5] HIPAA serves as a critical privacy floor and regulatory umbrella for most health information, whether accessed by a government agency, nongovernmental entity, or private business.

Under the Privacy Rule of HIPAA, protected health information (PHI) accessed by "covered entities" is highly regulated and controlled by the federal government.[6] PHI is described as any information that is held by a set of "covered entities" and which concerns an individual's health status, provision of care, and payment of care. Covered entities include health care providers, health plans (including government programs that pay for medical care), and health care clearinghouses (typically organizations that process and transfer data regarding PHI). Additionally, contracts made between covered entities

[4] 42 U.S.C. § 1320d, et seq.

[5] The Office of Civil Rights enforces HIPAA through complaints, compliance reviews and audits, and education and outreach to covered entities. Covered entities (including some government agencies) are required to comply with federal investigations and hearings regarding violations of HIPAA provisions.

[6] Please see Footnote 2 regarding the distinction between "protected health information" as defined by HIPAA and "personal medical information" contemplated in HB 14-1323.

and other organizations in order to carry out healthcare functions are regulated through mandatory "business associate agreements" that extend HIPAA's privacy requirements to the non-covered entity. Business Associate Agreements are a critical part of ensuring privacy is protected by any entity that can access PHI. A sample Business Associate Agreement can be found in Appendix E.

Covered entities and business associates must comply with HIPAA requirements to protect health information. Under HIPAA, covered entities can only use and disclose PHI: to the individual; for healthcare treatment, payment, and operations; for public interest and benefit activities; for research, public health, or health care operations; or pursuant to an otherwise permitted use and disclosure. While these broad categories are further defined under federal law and contain some detailed exceptions, any other uses or disclosures require the expressed authorization of the individual.

Organizations that access, store, and distribute electronic PHI must also adhere to HIPAA's Security Rule, which governs technical standards for PHI in electronic form. These agencies must demonstrate proper administrative, technical, and procedural safeguards are in place.

State laws that conflict with HIPAA are unenforceable unless they offer more stringent protections for personal privacy. 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, and adhering to requirements of regular audits.[7] In the event of an ambiguity between federal and state law, state agencies err on the side of caution and adhere to the more restrictive regulation.

B. 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

In the case of Medicaid applications based on health status, information received by the Department of Health Care Policy and Financing (HCPF) is provided directly from the applicant during the application process.[8] HCPF houses information during the eligibility determination process and upon approval, the information is subject to federal regulations, including HIPAA, to ensure it is secure.

[7] 45 C.F.R. § 164.530.

[8] This process does not include individuals who are applying to Medicaid solely on the basis of income- or age-based eligibility criteria. No health information is required to determine eligibility for these individuals and families.

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.

C. Data Surveillance & Analysis

Several state agencies have statutory authority to use health information to run program analysis and research, and to report out to the public their findings. All agencies have processes in place to ensure information is used appropriately under the law. For example, all information used for analysis is aggregated and de-identified before being reported to the public and shared to other parts of an agency. Data banks where health information resides are secure and audited by either the state or federal government to ensure privacy is protected.

The Colorado Department of Public Health and Environment's (CDPHE) mission is to protect and improve the health and environment of the people of Colorado. In furtherance of this mission, CDPHE operates over 200 applications including databases and registries, to monitor the prevalence of certain diseases in the population. Health providers are required by law to report limited amounts of information to allow CDPHE to access to certain health information for purposes of disease control and prevention. Several of these registries also house demographic information so that CDPHE can provide follow up services or investigate medical history, where appropriate.

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.

D. Regulatory Law Enforcement

Sometimes access to health information is necessary to enforce laws and regulations enacted for the purpose of promoting public health and safety. Investigating complaints against medical professionals, appealing denials of insurance coverage for medical procedures, prosecuting criminals, and ensuring proper tax collection represent some of the more significant reasons why accessing this information is important.

The Department of Regulatory Agencies (DORA) is dedicated to preserving the integrity of the marketplace and is committed to promoting a fair and competitive business environment in Colorado. Consumer protection is the mission of DORA, which houses nine separate divisions and the Executive Director's office. The divisions within DORA include Banking, Civil Rights, Consumer Counsel, Financial Services, Insurance, Professions and Occupations, Public Utilities Commission, Real Estate, and Securities. DORA's Divisions include over 40 boards, commissions and advisory committees. There are primarily three divisions within DORA, which may use and access health care information, including the Division of Professions and Occupations (DPO), the Civil Rights Division, and the Division of Insurance (DOI).

DORA boards within the Division of Professions and Occupations regulate licensed, certified and registered professionals. When statutes and rules governing a profession are violated, DORA boards and programs may take disciplinary action, including, but not limited to, letters of admonition, suspension, and revocation of licenses. To investigate these complaints, DORA boards and programs may require access to health care information. For example, if a patient desired to bring a complaint against a nurse, the patient would file a complaint with the Board of Nursing. The complaint form for health-related professions asks the complainant to sign an authorization for the release of medical records. The complaint form also notes that even absent this signed authorization, personal health information may still be obtained pursuant to the Board's statutory authority. This authority allows the Board to subpoena records to make determinations whether the appropriate standard of care was met. In this manner, boards and programs are able to fulfill statutory duties to protect the public.

The Civil Rights Division formulates policy and hears appeals in discrimination cases. If an individual files a complaint of discrimination with the Division on the basis of a disability, the complainant may be asked to provide more specific information about the disability status, including health information.

The Division of Insurance (DOI) regulates the insurance industry. Consumer Affairs section investigates consumer complaints against insurers to ensure compliance with Colorado laws and rules and adherence to policy contracts. The Division's financial operations ensure the solvency of the companies writing insurance contracts in Colorado. The Division's Licensing and Investigations unit ensures agents are properly licensed and investigates allegations of agent wrongdoings. Similar to DPO processes, if a consumer believes that a health insurance company has violated their rights, not paid for a covered benefit, or otherwise behaved inappropriately, they may file a complaint with DORA's DOI. Full investigation of a complaint, such as a denial of coverage for a desired service, requires detailed review of the reasons for the denial, which may require access to the patient's health information.

Although not addressed in this section, enforcement of criminal laws and non-regulatory civil violations can also rely on government access to personal medical information. Please see Appendix C for additional agency-specific examples related to law enforcement.

E. Government Employees

The Americans with Disabilities Act of 1990 (ADA), the Family and Medical Leave Act of 1993 (FMLA), and the Colorado Workers Compensation Act of 1915 each require health information to determine eligibility for some programs and benefits provided to state and local government employees. Each state agency's human resources office has a designated individual who is trained to manage this information properly and securely.

To access benefits provided under these laws, 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.

Health Information Use Example: State Employees
If a state employee was injured on the job and broke his leg, his human resources office would need to receive documentation of the injury from the employee and his or her doctor to determine if they would be eligible for compensation. That record is kept secure (via encryption or locked cabinet) and separate from his or her employment file.

As this scenario could then become a workers' compensation claim (regardless of whether the individual was a state employee), this information may also be shared with Colorado Department of Labor & Employment Division of Workers' Compensation to verify the information, process the claim, and provide reimbursement to the injured employee.

Another use for state employee health information is through the Colorado State Employee Assistance Program (C-SEAP), which provides direct counseling services to state employees in times of crisis. As a counseling provider, C-SEAP has identifiable health information, which is fully de-identified before reporting how state employees utilize services and before sharing with policymakers to demonstrate the efficacy of the program. C-SEAP does release individual medical information for the purpose of research and analysis to entities that are considered business associates under HIPAA (and who are thus under the regulations of HIPAA). A business associate agreement must be agreed upon before any information is shared.

Policies & Procedures for Ensuring Safe Access & Mitigating Risk

Access to health information is vital to day-to-day operations of many state agencies, and the 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.

All departments and non-governmental entities that were interviewed by the Task Force have administrative, physical, and technical safeguards in place to ensure security and privacy of health information. All agencies also have procedures in place ensure compliance with privacy laws and are subject to internal and external audits to ensure systems are in place to keep personal information secure. In addition, all agencies that share information with other agencies, across states, with researchers, and for claim processing, limit disclosure of only the minimum necessary information and on a need to know basis. No medical information is shared that is not relevant to the requests being made and permitted to be shared under state and/or federal law.

Several "best practices" were identified through the interviews, and many of these are common among industry organizations that have access to health information. These include:

- 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;

A. Security of Digital Health Information & Responding to Breach

Pursuant to HIPAA's Security Rule, which regulates the technical standards health information that is stored and accessed digitally, the Office of Information Technology supports information technology services for most state agencies and is responsible for technical and physical controls, as well as internal audits of those systems.

Some specialized state agencies and programs have additional security controls and are maintained separately. For example, HCPF's Medicaid Management Information System (MMIS) and support systems are not maintained by OIT, but HCPF has federally-required safeguards in place to secure electronic health information. Some state agencies with unique information technology systems needs as they relate to privacy, security, and health information data sharing maintain these systems through external vendors that have specialized knowledge of these systems. For example, DORA's Prescription Drug Monitoring Program (PDMP) is hosted and supported by an external vendor that provides PDMP solutions to multiple states, which enables authorized users to appropriately share information, even across state lines.

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.[10]

[10] C.R.S. § 6-1-716.

Concluding Summary & Recommendations for Next Steps

Throughout the Task Force's interviews, agencies and nongovernmental organizations provided strong examples of the ways in which they ensure the security and privacy of Coloradans' health information.

None of the interviewees identified a need for additional safeguards related to state and local government access to or use of health information. No entity reported that existing laws, regulations, or policies for accessing, using, and protecting health information were overly burdensome or redundant; however, Task Force members did express concern that additional regulations limiting access to such information could inhibit or prevent an agency's ability to fulfill its legal duties, encumber day-to-day operations, or increase costs for Colorado taxpayers. Overwhelmingly, Task Force members recognized the importance abiding by stringent procedures, and noted that within state and local government agencies, privacy guidelines are strict, well-known, and are respected by employees.

When asked how existing laws could be improved, many interviewees recognized that due to recent breaches of information in the public and private sector, privacy concerns are at an all-time high. Several agencies indicated that their staff spends a substantial amount of time fielding individual calls and inquires from the public regarding privacy concerns.

The Task Force recommends that any future legislative initiatives be aimed primarily at increasing public awareness and education around how their health information is used by state and local government agencies. Informing the public about the uses of health information would serve to improve public trust, as well as assist the effectiveness and efficiency of government operations.

Given these findings, the Task Force's primary recommendation is for the General Assembly to weigh several factors if statutory changes are considered regarding state and local government access to personal medical information. Namely, factors should include whether similar existing laws are in place, the extent to which the proposal creates additional administrative burden and expense, and how the public should be educated around the proposal.

APPENDIX A
List of Task Force Participants

Susan Beckman
Colorado Department of Human Services

Erin Benoy
University of Colorado

Cammie Blais
Connect for Health Colorado

David Blake
Colorado Department of Law

Kevin Bommer
Colorado Municipal League

Monica Bowers
Office of the State Auditor

Kim Burgess
Colorado Department of Personnel and Administration

Mary Caiati
Colorado Psychiatric Society

Amanda Chaney
Mental Health America of Colorado

Allan Chapman
Colorado Counties Incorporated & County Technical Services, Inc.

Ralph Gagliardi
Colorado Department of Public Safety

David Gallivan
Colorado Department of Labor and Employment

Ann Hause
Colorado Department of Public Health and Environment

Ronne Hines
Colorado Department of Regulatory Agencies

Kate Kiefert
Office of Governor John Hickenlooper

Jean Martin
COPIC

Elizabeth Mestas
Colorado Department of Corrections

Ben Price
Colorado Association of Health Plans

Christopher Underwood
Colorado Department of Health Care Policy and Financing

Lauren Victor
Colorado Department of Higher Education

Saskia Young
Colorado Department of Revenue

APPENDIX B
Task Force Interview Questions

Approved by the Task Force August 29, 2014

Questions for State & Local Government Entities

1. Please describe in general terms how your agency accesses, uses, or distributes personal medical information and for what specific purposes.

2. Does your agency access medical records for any of the following reasons:
   a. Employment-related requests, occurrences, or claims
   b. Individuals receiving health care services from your agency
   c. For data collection or analysis purposes
   d. To fulfill other statutory, regulatory, or mission-oriented obligations

3. For each reason to which you answered yes in number 2:
   a. Describe how the medical information is accessed, used, or distributed.
   b. Describe how the medical information is stored and protected.
   c. Please indicate whether access to personal medical information is mandatory or discretionary
   d. What are the specific state or federal laws, rules, regulations, or guidance that authorize your agency to access personal medical information?
   e. How does the agency determine if it is appropriate to access an individual's medical records?
   f. What is your basic procedure for ensuring patient privacy when accessing personal medical information?

4. Do all circumstances in which you access, distribute, or use personal medical information require an individual's consent?
   a. If yes, please indicate at what points consent is obtained.
   b. If no, in what circumstances is consent not required and why?
   c. In what circumstances is the individual's consent required? In what circumstances is consent not required?
   d. How is consent obtained, and for what period of time? Once? Ongoing?
   e. If your consent process differs based on the reason medical information is accessed, used, or distributed, please describe each process for obtaining and verifying consent and the circumstances in which consent is not required.

5. What are your agency's policies and procedures for accessing, using, or distributing personal medical information?
   a. Who is responsible for overseeing these policies and procedures?
   b. What type of education does your agency provide to employees regarding these policies and procedures?
   c. In what ways does your agency ensure these policies and procedures are observed and effectively enforced?
   d. What audit, breach, and remediation processes are in place?
   e. Please provide documentation of existing policies/procedures where possible.

6. Based on your experience, what additional safeguards or restrictions on access, use, or distribution are necessary to protect patient privacy or ensure compliance with HIPAA? Why?

7. Based on your experience, are there any unnecessary or overly-burdensome restrictions on access to personal medical information that should be limited or eliminated? Why?

8. Does your agency have any other recommendations for changes to current law, rules, or government practices that could improve protection of privacy?

9. Please describe the agency's policies and procedures for notifying the public of its privacy practices and ability to access, use, and distribute personal medical information?

10. What circumstances necessitate sharing personal medical information with other agencies?
    a. What procedures or agreements are in place to support these circumstances?
    b. Do these align with HIPAA releases of information?

Questions for Non-Governmental Entities

1. Please describe your organization's mission and experience with personal medical information.

2. Based on your experience, in general, what are your biggest concerns about ensuring personal medical information remains protected (internal or external to your organization)?
    a. What do you think is going well?
    b. What needs improvement?

3. In what ways do you interface with government agencies that access, use, and distribute personal medical information?

4. Are there circumstances in which your organization receives personal medical information from a governmental entity? If so, please describe.

5. Does your organization - or do your members - have best practices for ensuring patient privacy? Are you able to share these with the Task Force?

APPENDIX C
Individual Entity Report Summaries

Colorado Association of Health Plans (CAHP)

As a trade association, the CAHP does not exchange private information of any kind. However, the health insurance carriers we represent interface with various state agencies and as such, do exchange information.

Privacy Statutes and Regulations
The primary controlling privacy statute for health insurance carriers is HIPAA.

Policies and Procedures
Health insurers have a vested interest in ensuring covered individual's record privacy is maintained and that they are accessed only where appropriate. They also support the idea that patients have a right to know who records are shared with, and how they are shared.

Health insurance carriers follow HIPAA required procedures including security risk assessment for records stored in electronic format. Employees of health insurance carriers are trained in HIPAA policies and procedures and follow them.

Uses
Health insurance carrier use of private information is primarily related to the processing and payment of covered medical claims and medical management including coverage appeals. Carriers may exchange this data in HIPAA compliant fashion with various government agencies (i.e. HCPF).

Breach Procedures
Our members did not discuss breach procedures, but carriers would be compelled to follow HIPAA designated breach procedures.

Colorado Municipal League (CML)

County Respondents: Sterling, Monument, Winter Park, Berthoud, Lone Tree, Fort Morgan, Golden, Yampa, Platteville, Larkspur, Leadville, Arvada, Frederick, Breckenridge

Privacy Statutes and Regulations

The statutes and regulations cited by survey respondents were the Worker's Compensation Act, Americans with Disabilities Act, HIPAA, FMLA, and regulations enforced by the Colorado Department of Transportation.

Policies and Procedures

Efforts to ensure access to personal medical information is secure, limited, and appropriate most commonly included keeping information in a locked safe, drawer, or office, and often keeping medical information separate from other personnel information. Other precautions included: encrypting email messages and electronically stored documents, secure fax lines, password protection of electronic files, third-party secure websites, and double firewalls.

In a few cases, cities or towns indicated that consultation prior to accessing or sharing records was required. Many offered regular trainings on access to and use of private medical information, with heavy emphasis on HIPAA. The Town of Breckenridge referenced trainings available through the Mountain States Employer's Council and Society for Human Resources Management. Regular, internal audits were another mechanism used. The City of Fort Morgan referenced use of Business Associate Agreements (BAA) explicitly; it is likely that other entities also use BAAs because the HIPAA Privacy Rule requires them, and many entities referenced HIPAA as their primary controlling privacy law. Assuring employee knowledge of access and use policies permeated the survey responses, either through a personnel handbook, on the town or city's website, or through other means at the time of hire.

Obtaining consent from employees to access medical information was mixed; some cities and towns indicated that consent was needed for every instance, some stated that consent was not required for certain claims (such as worker's compensation and FMLA), and others said that consent was considered "ongoing" for the full term of employment.

Uses

Access to personal medical information is, in every instance, limited to employees of the city or town. For that reason, nearly every city or town indicated that its Human Resources Department had primary control over any collected personal medical information. Other departments or personnel with access to such information included: Town Clerk, Deputy Town Clerk, Town Board, Town Manager, Finance Director, Risk Management Department, and the Administrative Services Manager.

The most commonly cited use of private medical information was for processing worker's compensation claims. In case of a claim, information may or may not be accessed by the town or city at all, but is certainly shared with the city or town's worker's compensation insurance carrier (e.g. Pinnacol Assurance or the Colorado Intergovernmental Risk Sharing Agency – CIRSA – which insures many of Colorado's 271 municipalities). If an employee's provider recommends a work restriction, this restriction is shared with the employee's supervisor. Cities or towns sometimes retained claims for temporary or permanent disability accommodation or for leave under the FMLA.

Another common use of personal information was that needed for the employee to enroll in the city or town-provided health plan. However, with the exception of Fort Morgan, this information is aggregated before it is provided to the city or town. Fort Morgan indicated that it directly provides medical treatment to its employees. Many cities and towns require drug screenings and physical exams prior to hiring employees. Monument collects information related to substancC-abuse treatment. Platteville noted that

applicants to the Fire & Police Pension Association must provide medical records. Frederick requires new employees of the police department to pass a psychological exam.

Breach Procedures

Responses to procedures in case of breach were scant, either referring back to policies which prevent breach, citing HIPAA requirements, or indicating that such an event would be handled on a per-incident basis.

Other Comments

Few comments outside the above areas were discussed. No city or town indicated a need for more privacy regulations or a concern with current regulations.

Colorado Psychiatric Society (CPS)

Privacy Statutes and Regulations

In addition to following HIPAA requirements, which provide special protections for mental health information and substance abuse information, most psychiatrists follow the ethical code of the American Psychiatric Association (of which CPS is a chapter) which calls for even more rigorous standards. These ethical standards in key part always require patient consent for any release of medical information. While CPS itself does not have access to medical information, its members do.

Policies and Procedures

When a request for mental health records is made by an outside party (often a hospital or an agency such as Colorado Disability Determination Services (CDDS)), the psychiatrist will respond only when they know that consent from the patient has been obtained. They need not obtain consent themselves, but must be provided a release of information form signed by the patient which details the type of information requested by any entity requesting records. Often, disclosing original mental health/ medical records does not fulfill requests for information; rather summaries of the information requested are disclosed instead.

Uses

Generally, those entities, which seek this information, are university systems, hospitals (such as Denver Health), and other health care providers.

Breach Procedures

Breach procedures were not discussed during the interview.

Other Comments

In allowing access to medical records through electronic means, there ought to be special consideration of who can see the information as well as which information they can access. When a patient consents to their medical/mental health information being disclosed to another party, there should be clear delineation on the type and extent of information provided and the time frame from which medical information is needed. (e.g. the entire medical record for that patient vs. information for only a pertinent diagnosis; only information from a specific time period).

Mental health records are generally more sensitive than other medical records, and therefore should continue to benefit from more stringent protections.

In order to promote mental health treatment, barriers to seeking treatment must be broken down. One of these barriers is patient concern regarding whether this sensitive information will remain private.

Connect for Health Colorado (C4H)

The mission of Connect for Health Colorado is to increase access, affordability, and choice for individuals and small employers purchasing health insurance in Colorado.

Privacy Statutes and Regulations
The controlling privacy statute for C4H is HIPAA.

Policies and Procedures
C4H ensures that customers have clear power to either opt-in or opt-out of certain procedures. For example, customers were able to decide whether or not they wanted someone to call and follow up with them when they had a plan in their shopping cart but had not purchased the plan.

C4H must comply with MARS-E, which is a comprehensive guideline provided through the Centers for Medicare & Medicaid Services to ensure protection of sensitive data.

C4H's Transparency Policy lays out each individual and agency's responsibility to be in compliance with data protection mandates (both external and internal). Key points in the policy include: notification to the public regarding use of data; authority to use information is requested; individuals have a choice regarding how their information is used; individuals have the ability to view and correct records; who has access to information, how they use it, and how they protect it. Those who have provided consent to access personal medical information have the ability to revoke consent. Any new use of information requires C4H obtaining consent again.

C4H has a redress process for verifying accuracy of information, amending information, and to file complaints. C4H seeks to only access the minimum amount of information required to accomplish their goals, per HIPAA.

If applicants chose to apply for financial assistance, the Department of Health Care Policy and Financing can use or share the information if you or your family members apply for or already receive medical assistance with other program(s). The information can only be used for purposes of treatment, payment, determining eligibility, and other program and administrative operations or other purposes permitted by law. C4H will check applicant's answers using information in our electronic databases and the databases of partner agencies. If applicants are seeking financial assistance, C4H may ask you screening questions about their medical history to help C4H determine which assistance programs you are eligible for.

C4H and the Department of Health Care Policy and Financing (HCPF) are authorized to collect information on the application, including Social Security numbers, and will confirm information that may affect initial or ongoing eligibility for all persons listed on your application. Applicants allow C4H and the HCPF to use Social Security numbers and other information from your application to request and receive information or records to confirm the information in your application. You release Connect for Health Colorado and the Department of Health Care Policy and Financing from all liability for sharing this information with other agencies for this purpose. For example, C4H and the HCPF may get and share your information with any of the following agencies: Social Security Administration; Internal Revenue Service; United States Customs and Immigration Services; Department of Homeland Security; Centers for Medicare and Medicaid Services; Colorado Department of Labor and Employment; Financial institutions (banks, savings and loans, credit unions, insurance companies, etc.); child support enforcement agencies; employers; courts; and other federal or state agencies. C4H need this information to check applicant's eligibility for health insurance, help paying for health insurance and to give clients the best service possible if applicants choose to apply.

Exchanges must follow the Minimum Acceptable Risk Standards for Exchanges (MARS-e). The MARS-e takes information from the National Information of Standards and Technology 800-53 version 4 and adapted it to fit security requirements for the Healthcare Industry.

Uses

C4H does not collect medical information directly, but may be exposed to such information. The only information collected is demographic.

C4H often has to share data with others. They must report to the federal government (which is most often dC-identified data). They also interact with HCPF to ensure that enrollees are reconciled between the two systems, which requires sharing of enrollment information (e.g. income, number of people in household). This information comes from a HCPF database, which only contains information from people who have requested financial assistance, and the C4H enrollment system.

Breach Procedures

Breach procedures were not discussed. General comments on privacy can be found at http://connectforhealthco.com/sitC-information/privacy-policy/.

Other Comments

People feel vulnerable about government accessing and using information, particularly through a website, and C4H depends on consumer trust, therefore it is very important to ensure that this trust is being bolstered and maintained. It is for this reason that C4H has so many policies and procedures in place to ensure protection and appropriate use of personal information. Clear notifications on websites, and clear access for an individual to ask questions, is essential to promote consumer confidence.

COPIC

Privacy Statutes and Regulations

Because COPIC insures physicians, hospitals, and medical facilities for medical malpractice and provides legal defense coverage for certain regulatory proceedings, it is very interested in ensuring that patient records are kept private and only accessed where appropriate. COPIC itself is considered a business associate subject to HIPAA for certain risk management and other activities conducted on behalf of its insured.

Policies and Procedures

From a policy standpoint COPIC understands and supports the notion that patients should know how, and with whom, their records are shared.

COPIC has several procedures to ensure that private medical information (PMI) is kept private. One of these methods is performing a security risk assessment as required under HIPAA for entities maintaining medical records in an electronic format. Members of COPIC's workforce are trained in HIPAA policies; instructed to delete or destroy PMI stored on laptops or printed when it is no longer needed; and email-containing PMI is encrypted. Many COPIC employees dealing with PMI have medical backgrounds and/or licensure and, therefore, must abide by ethical duties to keep information private.

Once patients have filed a claim, their medical information related to the claim is no longer protected by physician-patient confidentiality. COPIC, however, continues to protect this information as appropriate pending resolution of the claim.

Uses

COPIC collects PMI in several ways: (1) it may have PMI from various sources related to a malpractice claim; (2) it may have PMI from an insured's patient when the patient and physician participate in the 3R's Program ("Recognize, Respond, and Resolve"). The 3Rs Program is an early intervention, patient-centered approach for addressing unexpected medical outcomes in a way that attempts to preserve the physician-patient relationship and reimburses the patient for related medical expenses.; (3) it may access some PMI as part of its risk management services for physician practices, hospitals, and other healthcare facilities; and (4) it may collect PMI related to an individual insured as part of its underwriting process.

Breach Procedures

Breach procedures were not discussed.

Other Comments

One question in terms of government access to private medical information relates to the application of the Prescription Drug Monitoring Program. Some questions that have yet to be resolved are: will patients be able to access the records collected through this program that are incorporated into the provider's medical record? Will providers be allowed to share this information for treatment purposes?

County Technical Services, Inc. (CTSI)

Privacy Statutes and Regulations

HIPAA, the Worker's Compensation Act, and regulations around reporting settlements to Medicare and adjudicating claims regulate CTSI's access to private medical information.

Policies and Procedures

Private medical information is only used for its intended business purpose. CTSI administers intergovernmental insurance pools for worker's compensation, property liability, automobiles, and health. These pools are considered governmental agencies.

To ensure that information is only accessed for its intended business purpose, CTSI uses encrypted email, uses dC-identified and aggregate information where possible (e.g. for underwriting purposes), and does not distribute personally identifiable information. CTSI also undergoes audits to ensure compliance with HIPAA, and trains employees in HIPAA compliance procedures.

Uses

The primary use of private medical information is for settling and adjudicating claims. Examples of this use include employment-related requests to verify Americans with Disabilities Act claims for reasonable accommodation, and processing worker's compensation claims.

Breach Procedures

Should a breach occur, CTSI follows the procedures required by HIPAA. Further, CTSI carries coverage in case of a breach.

Other Comments

The legislature needs to understand that everyone cannot be lumped together as "governmental" or "private" because there are so many intergovernmental agreements, and frequent information exchange between agencies. Agencies need latitude in access to information so they can properly execute their missions.

Department of Corrections

The Colorado Department of Corrections (DOC) is responsible for administering health care to all offenders at Colorado facilities. It stores protected health information (PHI) of all current and previously released offenders. Additionally, DOC's Human Resources uses PHI to adjudicate employment-related requests.

Statutes and Regulations

The Worker's Compensation Act, Family Medical Leave Act, American's with Disabilities, and state personnel procedures authorize DOC to access personal PHI to adjudicate employment related requests. C.R.S. 17-1-108, C.R.S 25-1-802.

As the medical provider for all offenders, DOC is considered a covered entity and subject to HIPAA regulations regarding PHI. DOC only releases the minimum information necessary and only on a need to know basis to another medical provider or if the offender signs an authorization to release PHI.

Policies and Procedures

Human Resources Director and management are responsible for managing employment related medical requests and ensuring privacy is maintained. Records of accommodations are kept separate from an employee's personal file and access is limited to a few trained staff. Staff is trained at the time of hire, annually, and as changes to regulations occurs. Medical information is kept separate from the employee's personnel file.

When offenders are transferred from facility to facility or require outside treatment, their medical file is sent with them.. DOC does have electronic health records of treatments received while incarcerated., but it does not, as of yet, have the ability to share this information electronically outside of the facility. In each facilities clinic there is a secure area for health record storage. The Office of Information Technology (OIT) monitors the electronic system.

Internal policies are updated annually, per regulation AR 950-02, which is related to ACA standard procedures for privacy. Employees are trained at hire and annually on privacy rules and regulations.

Uses

Human Resources

DOC uses Broadspire when adjudicating employment related workers compensation requests. All FMLA and workers compensation requests require information from the individual and their medical provider to make accommodations for employees. Information is provided on a voluntary basis and only information related to the claim is requested.

Healthcare for Offenders

DOC has access to PHI and provides healthcare to offenders in Colorado. Health records are generated in-house, both in electronic and hard copy. DOC shares PHI for three reasons. First, when offenders need specialty treatment from an outside care provider, the inmate's information is sent with them to the specialist. Second, is to ensure continuity of care for offenders transferring between facilities and once they are released from the correctional facility. When offenders are release from a facility, they have the ability to access their PHI generated during their incarceration. The offender owns the information and has access; the offender must give permission if access to their PHI is required (unless a court ordered is issued).. The third is statutorily obligated by C.S.R 103-1-104.5 and 183-4-15.5, HIV reporting and infectious disease reporting, respectively. That information is shared with the Colorado Department of Public Health and Environment.

Data Collection and Analysis
DOC reports aggregated PHI through DOC's Office of Planning and Analysis for request made by their stakeholders. For example, PHI is released for research, planning and numerous other purposes, and the information is dC-identified.

Breach Procedures
Because the DOC still stores most of the offenders personal medical information in paper form, security is monitored to ensure privacy is protected. OIT conducts audits at the request of DOC, to ensure compliance with laws and regulations.

Department of Health Care Policy and Financing

Statutes and Regulations

HCPF is authorized to access personal medical information through state and federal statutory regulations including HIPAA and Medicaid laws. HCPF is strictly regulated by federal regulations and is regularly audited by federal and state agencies to ensure compliance with both federal and state technology and HIPAA standards. Federal regulation is extremely restrictive and highly enforced. Proper protocols, controls, and procedures dictating the use of confidential data and information are in place.

Policies and Procedures

HCPF policies and federal regulations are regularly updated to meet changing technology needs. HCPF conducts extensive staff training on HIPAA requirements and its Department policies. Employees must receive annual training on how to protect client information. Data sharing is vital to the day-to-day operations and mission of HCPF. Personal medical information is used to determine eligibility for Medicaid, process payments and tailor services, control health care costs, and support university research. When information is shared between parties, emails and hard drives are encrypted to ensure security and privacy.

Uses

The vast majority of personal medical information (PMI) that HCPF is required to keep for their operations is related to program eligibility and provider payment. For example, applicants are required to provide name, address, social security number, household composition, income, and asset information. Providers are required to provide codes that describe the medical assistance provided. Generally, HCPF access to this information is limited under law to staff who are directly involved in the eligibility and payment systems controlled by the Department.

An example of how the Department uses confidential health information is illustrated in the Accountable Care Collaborative (ACC). Through regional centers, care is coordinated to ensure payment and treatments are being received and administered correctly. This system shares PMI between providers and care coordinators to ensure, for example, prescriptions are being prescribed correctly and do not conflict with previous diagnosis. This improves both quality of care and controls for costs. The providers and care coordinators are subject to the same federal requirements that ensure health providers keep client data confidential. Medicaid recipients have the opportunity to opt out of this system.

Additional HCPF staff are required by federal law to access this information to prevent provider fraud and client over-utilization. Adding further regulations by the state could make day-to-day operations in providing medical assistance through HCPF's programs unmanageable. The ability to prevent client over-utilization and provider fraud, and to improve health outcomes would be jeopardized by additional state regulation that differs from the rigorous existing federal requirements.

Breach Procedures

The Office of Civil Rights prosecutes any breaches of information or complaints by citizens.

Department of Higher Education

The Community College Campus System, Colorado State University, Colorado State University-Pueblo and the Auraria Campus were all respondents for DHE.

Statutes and Regulations

The Americans with Disabilities Act (ADA), Family and Medical Leave Act (FMLA) and Worker's Compensation authorize institutions and/or DHE to use personal medical information for employment-related requests and accommodations for students, staff and faculty. DHE and its institutions are also subject to Family Educational Rights and Privacy Act (FERPA), which protects student's records and privacy.

The institutions' health plans and health centers are considered covered entities and therefore are protected and subject to HIPAA regulations.

Policies and Procedures

For employment-related requests and accommodations, the individual seeking accommodations provides information and only what is pertinent to the claim is requested. The Human Resources division of the respective school is typically responsible for processing and approving these claims. Medical files are kept separate from personnel and student files. The division director is responsible for setting policy. Staff is trained upon hire, and are regularly updated and educated as needed, ensuring that privacy procedures are known and understood.

Uses

The institutions/DHE may access medical information when processing employment-related requests, handling accommodations or providing health care. Each respective department of a university may process ADA, FMLA, and Worker's Compensation requests from faculty and staff. Typically a department receives this information and then sends it to the university's human resources office for processing.

Each school's health care provider maintains, stores and accesses personal medical information. The majority of the information is stored in secured electronic records. Under HIPAA, the health care providers are authorized to use medical information for payment and operations. Access to personal medical information is limited to a need- to-know basis and only with the consent of the patient. Under state immunization requirements, institutions require access to student immunization records. Acknowledgement of HIPAA regulations is required at the point of service for those accessing a campus health center.

Colorado State University and Colorado State University-Pueblo may collect medical information for data and analysis purposes. Both use the collected data in support of effective operation and to ensure quality of care. Following protocol to ensure individual data privacy, all information is dC-identified and used in aggregate form for generalizable knowledge.

Breach Procedures

Breach procedures are available on each higher education institution's website.

Department of Human Services

The Department of Human Services (CDHS) has three offices, which administer health services and have access to personal medical information; the Office of Behavioral Health, the Office of Children, Youth and Families, and the Office of Community Access and Independence.

Statutes and Regulations

These offices administer direct health services and are thus considered a covered entity under HIPAA and subject to federal enforcement. Under C.R.S. 42, the sharing of personal medical information to parties other than the patient or medical provider is strictly prohibited unless direct consent is provided from the patient. CDHS is guided to operate under several state regulations.

Division	Best Practices
Behavioral Health	2 CCR 502-1
Division of Youth Corrections	2 CCR 504-1
Social Services	12 CCR 2509
Substance Abuse and Treatment	6 CCR 1008

While CDHS has remained compliant as a HIPAA Covered Entity, management of health information is inherently complex and made more so by the breadth of regulations related to it. Given that health information technologies represent a rapidly evolving facet of health care, CDHS will conduct ongoing review of the rules, statutes, and laws that apply to health information to ensure that they are current, understandable, concise, compliant, and properly limit access and use.

Policies and Procedures

Behavioral Health

Information collected while a patient is being treated at a Colorado Mental Health Institutes (CMHI), is securely stored in locked area, on encrypted devices and transmitted over secure networks. The CDHS HIPAA Officer, Compliance Officer, HIPAA liaisons, and CMHI management are responsible for ensuring staff is trained at the time of hire, annually, and as changes to regulations occur. Consent to access to medical information is general limited to 2 years.

Children, Youth and Families

Information collected while a patient is receiving treatment from the offices' facilities. All information is securely stored in locked area, on encrypted devices and transmitted over secure networks. The CDHS HIPAA Officer, Compliance Officer, HIPAA liaisons, and Children, Youth and Families management are responsible for ensuring staff is trained at the time of hire, annually, and as changes to regulations occur. Consent to access to medical information is general limited to 90 days, during the course of treatment, or when authorized by parents or guardians.

Community Access and Independence

Information collected while a patient is receiving treatment while a resident of the Veterans Community Living Centers. All information is securely stored in locked area, on encrypted devices and transmitted over secure networks. The CDHS HIPAA Officer, Compliance Officer, HIPAA liaisons, and Children, Youth and Families management are responsible for ensuring staff is trained at the time of hire, annually, and as changes to regulations occur. Consent to access to medical information is general limited to the length of stay or course of treatment.

Human Resources

Human Resources Director and management are responsible for managing employment related medical requests and ensuring privacy is maintained. Records of accommodations are kept separate from an

employee's personal file and access is limited to a small trained staff. Employees are trained at the time of hire, annually, and as changes to regulations occur.

Uses

Behavioral Health

CDHS provides direct care for individuals receiving mental health care in CMHI facilities. PMI is used for treatment, payment and operations. PMI is shared with CMHI when a patient is admitted to one of the regional facilities. PMI is generated throughout the stay and is shared only on a need to know basis. Receiving care facilities are given access to personal medical information to ensure continuity of care for patients. C.R.S. 42 part 2 and HIPAA regulate and authorize the use of medical information by CMHI, for the reasons discussed. Direct care information is provided to reporting agencies such as Center for Medicaid/Medicare Services (CMS) and the Veteran's Administration (VA) for accrediting, evaluation, and funding purposes. Patient consent is required, by HIPAA, for uses other than payment, treatment and operations. Information is used, in a dC-identified manner, for funding, oversight and program evaluation.

CHMI does not administer direct services for substance abuse treatment, but serves as an intermediary between patients and care, and thus shares PMI with treatment facilities per 6 CCR 1008.

Children, Youth and Family

The Office of Children, Youth and Family administers direct services to children in youth corrections facilities, children's welfare services, state funded nursing homes and those who are accessing state vocational rehabilitation services. These direct services are protected under HIPAA regulations and enforced by federal regulators. PMI is used for the purposes of treatment, payment and operations of the services provided by Children, Youth and Families.

Community Access and Independence

The Office of Community Access and Independence administers direct services to veterans and their spouses at the Community Living Centers those who are accessing state vocational rehabilitation services. These direct services are protected under HIPAA regulations and enforced by federal regulators. PMI is used for the purposes of treatment, payment and operations of the services provided by Community Access and Independence.

Human Resources

Internal Human Resources is responsible for administering medical related employment requests, including FMLA, ADA, and Worker's Compensations. All requests require information from the individual and their medical provider to make accommodations for employees. Information is provided on a voluntary basis and only information related to the claim is requested.

Breach Procedures

Breach procedures are regulated and audited by the federal government. The Compliance Officer and liaisons conduct the audits to ensure compliance and suggest additional steps to strengthen security (if necessary). CMHI, Veterans Community Living Centers, and Children, Youth and Families follow the HIPAA incident policy and incident assessment process when breaches occur. When a breach occurs, the Breach Notification Rule of HIPAA dictates that the breach must be reported to the Office of Civil Rights and reported to the public through multiple means (mail, C-mail, phone, and news sources).

Department of Law

The Department of Law (DOL) represents the State and State Departments in legal proceedings. Under certain circumstances, personal medical information is used to adjudicate claims in court.

Statutes and Regulations (that authorize the use of medical information)
Regulations, which authorize other agencies to access medical records, are used by the DOL to access personal medial information to litigate claims. Some departments provide medical treatment or pay for medical care, and the DOL may use that information in legal proceedings. Criminal statutes and civil rules of procedures control access to information pertinent to all legal proceedings.

During litigation, DOL refers to the stricter of state and federal laws to guide how they can gain access to personal medical information. Additionally, uses and disclosures of personal medical information pursuant to court order or other exceptions are authorized under HIPAA. Mental health and substance abuse recordscan only be gained through direct consent or court order, under HIPAA for mental health treatment records and per 42 C.F.R, part two for substance abuse treatment records.

Policies and Procedures (on how medical information is protected)
All individual cases are stored on protected servers and access is limited to the parties to a claim and their lawyers. All servers are protected and subject to HIPAA compliance and security regulations. OIT works with DOL to ensure their servers are secure. Access to personal medical information by DOL is not direct. Access is only gained on behalf of a client, for legal proceedings.

Uses of medical information
Personal medical information is used by DOL when it is pertinent to representing their clients in litigation and to respond to legal inquiries from clients. Almost every division in DOL receives some sort of medical information to perform their official functions. Identifying information is often material to the case and is required to be available to the court. If medical information is material and relevant to a proceeding, the court can obtain access to PMI.

Internal Human Resources is responsible for administering medical related employment requests, including FMLA, ADA, and Worker's Compensation. All requests require information from the individual and their medical provider to make accommodations for employees. Information is provided on a voluntary basis and only information related to the claim is requested.

Department of Labor and Employment

The Department of Labor and Employment (DOLE) is responsible for administering and adjudicating employment related issues (such as worker's compensation and unemployment insurance) in the state.

Statute and Regulations
The Colorado Worker's Compensation Act and the Colorado Unemployment Act provide the legal framework for why DOLE can access personal medical information to adjudicate claims.

Policies and Procedures
All documents related to employment related requests that DOLE receives are stored only in hard copy in a secure file room. All employees are trained upon hire and when needed in privacy rules and regulations.

Access to medical information is mandatory for any party who is seeking benefits. In order to determine if the employee is eligible for a benefit, only information that is related to the request is required by the DOLE. Access to information in these claims is limited to the parties, those with approval from the employee, and through judicial review.

HIPAA regulations allow states to access medical information and administer worker's compensations processes. Internally DOLE follows similarly restrictive regulations regarding privacy and personal medical information.

Uses
Access to medical information is limited to adjudicating claims for employment related requests, primarily worker's compensation and rarely in the unemployment system. DOLE is responsible for adjudicating these claims for all employees in the state of Colorado.

The employee and their medical provider compile the medical information pertinent to the claim and provide it to their employer, which is then processed by DOLE. On some occasions, the Industrial Claims Appeals Office (ICAO) uses this information, which is responsible for the appeals process for workers compensation and unemployment benefits.

Breach Procedures
DOLE follows statewide protocols regarding breach procedures. Because all records are kept in hard copy only, there are no breach procedures regarding electronic storage. Individuals to the claim are informed of any breaches during their claims process.

Department of Personnel and Administration

Statutes and Regulations

The State Personnel Director is charged with administration and management of the state employee's group health plans. Employees in the Employee Benefits Unit of DPA are authorized by federal law to access personal medical information for the purposes of treatment, payment, and health care operations. This access is governed by HIPAA and policies and procedures are in place to ensure the confidentiality of the information. Additionally, DPA contracts with health providers and requires that these providers strictly comply with HIPAA requirements.

The Colorado State Employee Assistance Program (C-SEAP) is considered a health care provider and is therefore a covered entity under HIPAA and subject to federal regulations. The Standard Operating Procedures mirror the regulations covered in HIPAA and ensure that patient privacy. [12] C.R.S. § 24-50-604 states, that C-SEAP "address personal problems and workplace issues faced by state employees and employers before the problems and issues severely impact the productivity, safety, work relationships, absenteeism, and accident rates of state employees in the workplace."

Regarding worker's compensation, the Colorado Worker's Compensation Act guides and allows access to personal medical information pertinent to the employees claim.

Policies and Procedures

The medical information generated during treatment with C-SEAP is stored electronically in a secure database and secure drive. Access to medical information is restricted to C-SEAP staff members only. Medical information generated during treatment is kept on secure servers for an additional 10 years after treatment, before being destroyed.

The C-SEAP director is responsible for overseeing the policies and procedures[13]. All new employees are train upon hire and receive annual training on state regulations and HIPAA policies.

For worker's compensation, family medical leave determinations, and administration of the American's with Disabilities Act as Amended (ADAAA), all records are maintained electronically and kept separate from the employees personnel file. Access is limited and password protected.

Uses

Colorado State Employee Assistance Program

C-SEAP provides direct counseling services to state employees in nine offices located throughout Colorado by C-SEAP's staff of licensed mental health professionals, or by graduate students practicing under the supervision of one of C-SEAP's licensed mental health professionals. C-SEAP will release medical information/medical records to the client or to a third party only upon receipt of a written (and verified) Release of Information signed by the client/employee. This process is strictly monitored by C-SEAP. There is no billing associated with C-SEAP services; all services are free of charge to state employees.

C-SEAP manages the Psychological Fitness for Duties assessments for state agencies. Evaluations are shared only with the consent of the individual. All records of the PFD are stored by C-SEAP and protected in a secure server.

[12] C-SEAP/DPA Standard Operating Procedures 003A, 004, 005, 007A, 009, 013A, 014A, and 015A are relevant to enforce department policies pertaining to personal medical information and are available upon request from DPA.
[13] The Director of C-SEAP also currently serves as the HIPAA Privacy Officer

C-SEAP accesses medical information in order to provide state government leaders with dC-identified aggregate information to demonstrate program efficacy and use. Additionally, C-SEAP does share aggregate data with research facilities that sign a business associate agreement (making them compliant to HIPAA regulations).

Worker's Compensation
DPAP also access medical information for the purposes of workers compensation as a part of their risk management. This action is administered through a third-party administrator who accesses the claim information. The employee seeking benefits provides all information in the claim and only what is pertinent to the claim is required to be in the report.

Breach Procedures
The Office of Information Technology performs audits to ensure the servers are secure.

Department of Public Health and Environment

The Colorado Department of Public Health and Environment (CDPHE) accesses and uses personal medical information generally for its work for public health purposes. Pursuant to the federal Health Information Portability and Accountability Act (HIPAA), CDPHE operates as a public health authority in its access to and use and disclosure of personal health information. Multiple types of providers and/or regulated entities are required by law to either report medical information to CDPHE, or allow CDPHE to have access to their medical records for public health purposes, such as to track diseases concerning to the public's health, report occurrences in health care facilities, and collect birth and death information. The focus of public health work is on population health, not individual health care, and as such CDPHE collects both identified and unidentified information to track and measure population health.

Statutes and Regulations

CDPHE operates multiple health related programs, which use personal medical information for daily operations related to federal and state statutory and regulatory requirements. The following table summarizes the authorities that require or permit CDPHE's programs to access personal medical information.

Program	Statutes and Regulations
Disease reporting and investigations	General reporting and investigation authority: § 25-1-122, C.R.S. and 6 CCR 1009-1 Tuberculosis: §25-4-501 *et seq*., C.R.S. HIV/AIDS: §25-4-1401 *et seq*., C.R.S. and 6 CCR 1009-9
Newborn metabolic screening	§25-4-1004(b), C.R.S. and 6 CCR 1009-25-4-1007
Colorado Responds to Children with Special Needs	25-1.5-102(1)(r), C.R.S. and 6 CCR 1009-7
Vital Statistics (birth, death, marriage, etc.)	§25-2-101 *et seq*., C.R.S. and 5 CCR 1006-1
Cancer reporting	§25-1.5-101(1)(q), C.R.S. and 6 CCR 1009-3
Immunization reporting	§25-4-2401 *et seq*, C.R.S.
Health facility inspections	§ 25-1-124, C.R.S. and multiple chapters in 6 CCR 1011-1
Radiation	§ § 25-1.5-101(1)(k) and 25-11-104, C.R.S. and 6 CCR 1007-1, Sections 4.6, 4.18 and 4.56
Trauma	Designation, § 25-3.5-704(2)(d), C.R.S. and 6 CCR 1015-4, Ch. 3 Registry, § 25-3.5-704(2)(f), C.R.S. and 6 CCR 1015-4, Ch. 1
Emergency Medical Services	Provider investigations, §25-3.5-205(4), C.R.S. and 6 CCR 1015-3, Ch. 1 EMS data collection, § 25-3.5-501, C.R.S. and 6 CCR 1015-3, Ch. 3
Blood/lead screening	Environmental and Chronic Diseases 6 CCR 1009-7
Newborn hearing screenings	§ 25-4-1004.7, C.R.S. and 6 CCR 1009-7
Old Age Pension Dental Assistance	§25-21-104(2)(a)(II)(d) and §25-21-106, C.R.S.
School-Based Health Centers	Centers for Disease Control and Prevention (CDC) reporting requirement to provide unduplicated child level and aggregate data, Health Resources and Services Administration (HRSA) reporting requirement to provide unduplicated aggregate data

Policies and Procedures

CDPHE has adopted 37 department policies that pertain to privacy and security. These policies require employees to take all necessary and proper precautions to appropriately protect confidentiality in their day-to-day use of confidential information. The policies also require that only the minimum information necessary to accomplish the task at hand shall be collected, created, received, amended or maintained. In addition, only the minimum necessary number of people shall be given access to sensitive information, taking into account staff-assigned duties, backup routines and the optimal workflow of the unit.

Three of the CDPHE policies are particularly relevant to the protection of personal medical information. Specifically, Policy 10.37 - Confidentiality, pertains to employee requirements as it covers collection, use, access and disclosure. Policy 15.27 - Data Privacy and Security, covers minimum necessary use, data release requirements and physical security, and Policy 15.17 - Access Control, addresses technical security.

Uses

CDPHE is responsible for many health related programs that monitor, collect, and analyze medical information data, including disease reporting and investigation, screening and prevention services, vital statistics reporting, health facility and emergency medical services and trauma programs, and laboratory services. Personal health information is used and disclosed only for purposes consistent with the mission and authorizing rules and statutes of CDPHE and the practice of public health. Program managers ensure that personal health information is neither used internally nor disclosed to an external party for a purpose that is in violation of the department's mission, rules and statutes. Information requests are reviewed and amended if it is found that some part of the information requested is no longer needed or exceeds minimum necessary access guidelines. Moreover, program managers must be prepared to document how any use or disclosure is a permitted use and disclosure, in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or other statute or rule. Any public reporting of public health data maintained by CDPHE is done at the aggregate (dC-identified) level. Several of CDPHE's programs may use reported disease information to offer resources or access to care and treatment services, which the client may choose to decline.

Breach Procedures

CDPHE policies 15.6, Reporting Potential Problems in Privacy and Security, and 15.7, Incident Response, set forth the policies and procedures to be followed in the event of a privacy or security breach. Upon receiving a report of a potential privacy or security breach, CDPHE's privacy offer and security officer work collaboratively with the program reporting the incident and CDPHE's Office of Legal and Regulatory Compliance to determine both what steps are necessary to mitigate, if possible, the breach, and whether notice of the breach to any potentially impacted individuals is required. CDPHE's privacy officer also makes recommendations for additional measures to prevent any such future breaches, where appropriate.

Department of Public Safety

The Department of Public Safety (CDPS) has access to personal medical information as it relates to employment related requests, fitness for duty, and for meeting immediate medical needs of disaster victims.

Statutes and Regulations

The Workers Compensation Act, the Family and Medical Leave Act, and the Americans with Disabilities Act authorize CDPS access to medical information as it relates to benefit claims. State personnel rules authorize the use of PMI to determine employee fitness for duty. PMI may also used to determine access to national security information.

Policies and Procedures

Human Resources Director and management are responsible for managing employment related medical requests and ensuring privacy is maintained. Records of accommodations are kept separate from an employee's personal file and access is limited to a small trained staff. Staff is trained at the time of hire, annually, and as changes to regulations occur. Claims are processed through a chain of command and are processed through the Human Resources Department of CDPS.

Uses

CDPS uses PMI only when an employee is seeking an accommodation or approval of being fit for duty. Internal Human Resources is responsible for administering medical related employment requests, including FMLA, ADA, and Worker's Compensations. All requests require information from the individual and their medical provider to make accommodations for employees. Information is provided on a voluntary basis and only information related to the claim is requested. Only information that is pertinent to the claim is required to administer the accommodation or approve return to work requests.

CDPS often works with the Colorado State Employee Assistance Program (C-SEAP) when psychological fits for duty assessments are required. Information provided to CDPS contains no specific detail of the assessment, only whether the psychologist approves an employee's fitness for duty.

Breach Procedures

Files containing PMI are kept separate from personnel files and access to files is at the discretion of the employee and the human resources director.

Circumstances outside employment environment

The Division of Homeland Security and Emergency Management (DHSEM), within the CDPS, does not collect medical information directly, but has access to such information during disasters for victims with special medical needs. DHSEM is not the custodian of the records; instead it has an agreement with the Federal Emergency Management Agency to maintain those records in a manner consistent with federal privacy laws, including the federal Health Information Portability and Accountability Act.

Regarding the access to and use of information outside the employment environment, CDPS employees obtain, use and store medical information in fulfillment of their statutory responsibilities either from written consent or by relevant court order. In times of emergency, disaster or homeland security investigations where federal agencies aren't the custodian of information, those processes still apply in addition to the authority given under public health statutes, enforcement of quarantine orders and/or Governor's Executive orders in a declared emergency. In all of those circumstances the information would be stored, managed, and held under the confidentiality that exists within Criminal Justice Records.

Department of Regulatory Agencies

The Department of Regulatory Agencies (DORA) is dedicated to preserving the integrity of the marketplace and is committed to promoting a fair and competitive business environment in Colorado. Consumer protection is the mission of DORA, which houses nine separate divisions and the Executive Director's office. The divisions within DORA are: Banking, Civil Rights, Consumer Counsel, Financial Services, Insurance, Professions and Occupations, Public Utilities Commission, Real Estate, and Securities. DORA's Divisions include over 40 boards, commissions and advisory committees. Within DORA**, t**here are primarily three divisions, which may use and access medical information, including the Division of Professions and Occupations (DPO), the Civil Rights Division, and the Division of Insurance as highlighted below:

Statutes and Regulations

Division of Professions and Occupations: *Business and Inspections Branch*

Board	Regulation
Barbers and Cosmetology	28 CFR Part 35, ADA
Boxing	Director/Commission Rule 3.2, 3.3, and 3.4
Accountancy	28 CFR Part 35, ADA ; Board Rules: 3.6 A.5., 6.14 ,7.5
Electrical	28 CFR Part 35, ADA
Plumbing	28 CFR Part 35, ADA
Architects, Engineers and Land Surveyors	28 CFR Part 35, ADA
Landscape Architects	28 CFR Part 35, ADA

Division of Professions and Occupations: *Health Care Branch*[14]

Board	Regulation
Acupuncture	§§ 12-29.5-110(1)(f), 12-29.5-106(3)(a), C.R.S. 42 CFR Part 2
Athletic Trainers	§§ 12-29.7-109, 110, C.R.S.
Audiology	§§ 12-29.9-109(3), C.R.S.
Chiropractic	§§12-33-119(7), 12-33-117.5, C.R.S.
Dentistry	§§ 12-35-109(1),(2), 12-35-129(1)(z), 12-35-129.2(2), 12-35-129.2(7)(c)(II) and (d), C.R.S.
Hearing Aide Providers	§ 12-5.5-301(3), C.R.S.
Massage Therapists	§§ 12-35.5.112 (b) & (c), 12-35.5-114, C.R.S.
Medical	§§ 13-90-107(1)(d)(III)(C), 12-36-104((1)(b),(3), 12-36-118, 12-35.5-101 et seq. C.R.S.; Board Policy 10-16; 42 CFR Part 2
Mental Health	§§ 12-43-221 (1)(b)(III), 12-43-221, 12-43-224, C.R.S.; 42 CFR Part 2
Midwives	§ 12-37-107(6), C.R.S.
Naturopathic Doctors	§§ 12-37.3-104, 12-37.3-112, C.R.S.
Nursing	Nurses Practice Act - §§ 12-38-111(1)(a); (3); 12-38-112(1)(a); (3); 12-38-112.5(4), (8); 12-38-116.5(4)(c)(III)(A);(7);(8)(a),(b),(c),&(d);(13)(a); 12-38-117(1)(c),(f),(h),(i),&(j); and 12-38-131(5), C.R.S. Nurse Aide Practice Act – §§ 12-38.1-111(1)(i), (j), & (k); 12-38.1-113(1); (1)(p); (2)(a); (3); and 12-38.1-113(5), C.R.S. Psychiatric Technician Practice Act – §§ 12-42-113(1)(i) & (j); 12-42-115.3, C.R.S. - which refers back to

[14] 28 CFR Part 35, ADA is applicable to any Healthcare board where accommodations may be required for licensure examination.

	§ 12-38-116.5, C.R.S. (as listed above).
Nursing Home Administrators	§§ 12-39-105(V), 12-39-113, C.R.S. 42 CFR Part 2
Occupational Therapists	§ 12-40.5-110, C.R.S.
Optometry	§§ 12-40-107(1)(m), 12-40-118.5, C.R.S., 42 CFR Part 2
PDMP	§§ 12-42.5-404, 406, C.R.S.
Pharmacy	§§ 12-42.5-106, 120 and 131, C.R.S.
Physical Therapists	§§ 12-41-103.6(2), 12-41-115(1)(f), 12-41-117(5), 12-41-201(1)(d), 12-41-201(2), 12-41-210(1)(d), and 12-41-212(4), C.R.S.
Podiatry	§§ 12-40-107(1)(m), 12-40-118.5, C.R.S., 42 CFR Part 2
Respiratory Therapists	§ 12-41.5-109 (5.5)(b)(II) & (III), C.R.S.
Speech Language Pathologists	§§ 13-90-107(1)(d)(III)(C), 12-43.7-102,12-43.7-111, C.R.S., 42 CFR Part 2
Surgical Assistants/Technologists	§12-43.2-105(6)(b)(II) & (III), C.R.S.
Veterinary	§§ 12-64-105(9)(e), 12-64-120(3), 24-72-204(3)(a)(XIV), C.R.S.

Civil Rights Division

Commission	Regulation
Civil Rights Division	Title 24, Article 34; § 24-34-306(2)

Division of Insurance

	Regulation
Consumer Affairs; Investigations and Licensing; Senior Health Insurance Program (SHIP)/Senior Medicaid Patrol (SMP)	Title 10, C.R.S.

Policies and Procedures

In general, all medical information is held confidential in accordance with Title 24, the Administrative Procedures Act. In addition, the public does not have unrestricted or unmonitored access to DORA's work environment and medical information is maintained within secure electronic or hard case copy files with the Department. Electronic records are encrypted and otherwise secured with the support of the Office of Information Technology.

In many instances, the complaining party, applicant for licensure, or applicant for services obtains medical information. These instances do not require consent, and may be as part of a request for an accommodation varying in nature. In instances where medical information is reviewed by staff, boards or commissions, the individuals are trained to understand the nature of the privacy laws, complying with the Colorado Open Records Act, the organic practice act, other applicable statutes, and the Open Meetings Law. Several of the boards are closed to the public, further ensuring privacy of medical information. Access to medical information is only granted to parties to the claim.

Uses

In DPO, boards and programs are responsible for overseeing licensing professions in the state of Colorado. These boards/programs license certify and register professionals; and may impose discipline of professionals. In the protection of consumers, the boards/programs may access information as part of the application, complaint or disciplinary process pursuant to the practice acts. Generally, specific regulations allow boards/programs to investigate complaints, issue subpoenas and to compel the production of evidence, including medical information. For example, the Board of Nursing may compel medical records to be produced to determine whether the nurse met the standard of care.

In the Division of Insurance, the Consumer Affairs section investigates consumer complaints against insurers to ensure compliance with Colorado laws and rules and adherence to policy contracts. The Licensing and Investigations unit ensures producers are properly licensed and investigates allegations of agent wrongdoings.

The Civil Rights Division formulates policy and hears appeals in discrimination cases. If an individual files a complaint of discrimination with the Division on the basis of a disability, the complainant may be asked to provide more specific information about the disability status, including health information.

Breach Procedures

All staff and members of boards are trained in privacy regulations, including HIPAA and hold medical information as confidential in accordance with Title 24, the Administrative Procedures Act. The Division of Professions and Occupations adopted Division Policy 80-16, where program administrators/directors provide education and oversees enforcement of confidential information.

Department of Revenue

The Department of Revenue (DOR or Department) is comprised of four divisions: Division of Tax, Division of Enforcement, Colorado Lottery Division and the Division of Motor Vehicles (DMV). Of those divisions only the Division of Tax, DMV and the Department's Human Resources section utilize personal medical information.

Statutes and Regulations

Division of Tax

DOR operates under full compliance with HIPAA regulations for purposes of tax audits. DOR is authorized to conduct tax audits through C.R.S. 39-21-113(4)(a), (6). During tax audits, medical information may be used to verify the correctness of claims. In these instances, all personal identifying information (PPI) is redacted. In addition, section 24-72-602(3) of HB14-1323 specifically states that it does not prohibit the Department from accessing an invoice, a sales receipt, or other documentation of a sale necessary to substantiate an exemption from state sales tax under section 39-26-717, so long as no PPI or medical information is contained in that documentation.

Division of Motor Vehicles

C.S.R 42-2-111, 42-2-116, 42-3-204, 42-4-1208 authorize the DMV to use medical information in certain circumstances. Individuals seeking accommodations and their physicians provide all medical information voluntarily and only information relevant to the requested accommodation is collected. The Driver's Protection Privacy Record of 1994, U.S.C. 2725 protects all personal medical information collected by the DMV to determine accommodation eligibility.

Human Resources

DOR's Human Resources follows HIPAA regulations to ensure employee privacy when accessing employment-related requests, such as ADA and FMLA.

Policies and Procedures

Division of Tax

The Division of Tax trains auditors in privacy procedures and laws, including HIPAA and Colorado's tax confidentiality statute, C.R.S. 39-21-112. In addition, auditors are monitored by supervisors to ensure consistent practice of privacy protocol.

Division of Motor Vehicles

The DMV follows the guidelines of the 1994 Driver's Protection Privacy Record's Act and internal procedures, which are reviewed annually by DMV operation directors. Employees are given Driver's Privacy Protection Act Training when hired and annually thereafter. All records containing medical information to determine eligibility for medical accommodations are stored separately from drivers' records. Access to this information is granted on a need-to-know basis. The county clerks and recorders serve as DOR's authorized agents for title and registration transactions as set forth in Article X Section 6 of the Colorado Constitution and C.R.S. 42-1-210(1) and are subject to the same confidentiality requirements.

Human Resources Section

DOR's human resources section ensures that worker-related requests, including worker's compensation, FMLA, and ADA accommodations are protected. Files that include medical information are kept separate from the individual employee files with access to these files limited.

Uses

Division of Tax

Access to information for auditing purposes is mandated by C.R.S. 39-21-112. However, in addition to HIPAA compliance, Colorado's tax confidentiality statute, C.R.S. 39-26-717, strictly prohibits sharing tax information. Both of these statutes ensure compliance of privacy standards for personal information, including medical information. In addition, it is important to note that the tax division accepts the judgment of the medical provider if medical necessity is a criterion for exemption.

The field audit program reviews books and records of taxpayers to verify the correct amount of tax was collected and remitted to the state. When reviewing a medical office, field auditors may come in to contact with medical information to determine: (1) that a tangible personal property (TPP) was transferred to the patient, and (2) that the TPP is exempt from taxes. These audits operate under full compliance with HIPAA regulations and state statutes regarding tax confidentiality. As such, personal medical information is not included in the auditing process, as individual permission is required to access those details. Additionally, the business provides the records which are not distributed outside the auditing process.

Division of Motor Vehicles

The DMV is comprised of two entities: (1) vehicle services, which include titles and registrations, and (2) driver services, which include driver licenses. Individuals applying for limited physical impairment accommodation and renewal of handicap provisions must provide documentation of the disability. Applicants must use a DR 2219 (Persons With Disabilities Parking Privileges Applications) to request accommodations. Medical information, which specifies if the disability is temporary or permanent is provided to the Division of Motor Vehicles in Form DR 2219 and is verified by the individual's physician. Only a limited amount of information is requested by the DMV to verify accommodations requests.

Vehicle Services

All medical information provided to verify title and registration accommodations is held in the Colorado State Title and Registration System (CSTARS) to establish what accommodation the applicant can receive. The image of Form DR 2219 is scanned and maintained in DOR's server. Peace Officers, county clerks, and title and registration section staff who are verifying titles and registration accommodations have access to FormDR 2219, 42-3-204 7b

Driver Services

Under the DMV's driver's license (DL) section, C.R.S. 42-1-111 authorizes the collection of medical information to support sight, physical and or mental abilities after failing to pass these requirements during the licensing issuance or due to receipt of report from a law enforcement officer. Similar to titles and registrations, DL requests applicants and their medical providers to fill out Form DR 2401, which a DL office manager verifies. This form is digitally filed, but not attached the applicant's driving file. Access is highly restricted. C.S.R 42-2-116 authorizes the DMV to place special conditions or restrictions on driving through this form. The DL also requires medical information to complete gender change status applications with form DR 2038. These requests must be completed by the physician and are treated the same as a DR 2401 request.

Breach Procedures

The Office of Information Technology is responsible for the technology services used by the Department of Revenue. It is important to note that although HB14-1323 expressly addresses DOR, the Department's processes and procedures for accessing personal medical information continue to be in compliance with the statutory requirements set forth in HB14-1323 since the Department has always operated in compliance with HIPAA.

Mental Health America – Colorado (MHA)

Privacy Statutes and Regulations

No privacy statutes or regulations were discussed specifically, with exception to cursory mention of HIPAA.

Policies and Procedures

A licensed social worker collects the completed intake form, which contains limited private medical information. Any hard copies of the information are kept in a limited access, locked cabinet. Electronic information is kept on a password-protected computer, and files are not saved to the shared drive. If asked for patient information by someone other than the client and without patient consent, MHA will neither confirm nor deny that they have any records at all for the patient.

Uses

MHA works, in part, to connect people with free mental health services through a network of pro bono therapists. To connect patients with therapists, patients fill out a simple intake form which contains identifiable information and some medical information, such as a history of mental health illness and treatment. Once the patient is connected with a therapist, the therapist keeps any ongoing medical records. Intake forms are kept at MHA in case the patient needs a new therapist, additional services, or other needs arise.

Breach Procedures

Breach procedures were not discussed.

Other Comments

There is a severe stigma surrounding mental health treatment, and an important piece of that stigma is the possibility that information may be shared or accessed without patient consent or control. This concern, though unfounded, is so deep seated that it works to prevent people from seeking mental health services. Anything that can increase transparency regarding how and when this information is used, and any educational pursuits that can inform people regarding their rights and how they can access their own information, will help to erode this stigma.

Office of the State Auditor (OSA)

The Office of the State Auditor (OSA) is a constitutionally created, independent government agency that was established to promote operational efficiency and to ensure accountability of government agencies. The Colorado Constitution provides the State Auditor with the authority "to conduct postaudits of all financial transactions and accounts kept by or for all departments, offices, agencies, and institutions of state government...and to perform related duties with respect to such political subdivisions of the state as shall be required by law." In addition to conducting performance and financial audits of all state agencies, departments, and institutions, the OSA oversees audits conducted by independent audit firms of all of Colorado's local government entities.

Privacy Statutes and Regulations

C.R.S. § 2-3-107(2)(a) authorizes the State Auditor to access agency records for the purpose of conducting audits, and explicitly allows access to records, which would otherwise be confidential.

Policies and Procedures

Prior to requesting information from an agency, in accordance with C.R.S. § 2-3-107(2)(a), the Office of the State Auditor (OSA) will determine the necessity of accessing personal identifying health information to achieve the audit objectives. Whenever such access is not needed to accomplish the audit objectives, the OSA does not request the information. When personal medical information is requested from an agency, the OSA instructs the agency to relay the information through a secure protocol, if relayed electronically, or on an encrypted disc or portable drive. The OSA does not deal frequently with paper files, but when it does, the files are kept in locked trunks.

Once the OSA has received information, it is maintained in encrypted formats and/or on limited-access drives so that only the auditors assigned to that particular audit may access the data during the audit. For reporting audit results, data are aggregated such that no identifiable information is included in the final report. All information collected and incorporated into work papers is confidential under statute (C.R.S. § 2-3-107(2)(b). At the conclusion of the audit, any protected data needed to support the audit findings is saved in an encrypted format in the electronic audit files. All other protected data and other formats are destroyed in accordance with the OSA Security Policy. Though the Legislative Audit Committee may approve a request that underlying records to an audit report be released publicly, the Committee has never done so and cannot release information required by law to be kept confidential.

All OSA employees are required to annually attest that they have read and agree to adhere to the OSA's Information Security Policy and all applicable statutes. Applicable statutes include C.R.S. § 2-3-103(3) which states: "The work papers of the Office of the State Auditor shall be open to public inspection only upon approval of a majority of the members of the [Legislative Audit] Committee. Only the specific work papers that the Committee votes to approve for disclosure shall be open to public inspection. Work papers that have not been specifically approved for disclosure by a majority vote of the Committee shall remain confidential;" C.R.S. § 2-3-107(2)(b) which states: Notwithstanding the approval of the [Legislative Audit] Committee to release the work papers of the Office of the State Auditor…, no information required to be kept confidential pursuant to any other law shall be released in connection with an audit" and C.R.S. § 2-3-103.7, which states: "Any state employee or other individual acting in an oversight role … who willfully and knowingly discloses the contents of any report … by the [OSA] prior to release of such report by a majority vote of the [Legislative Audit] Committee is guilty of a misdemeanor …"

In addition, trainings on the Information Security Policy are conducted for every new staff member, every two years for current employees, and for all staff whenever the policy has changed.

Uses

The OSA regularly accesses private health information in order to conduct audits of state agencies in accordance with the Colorado Constitution and statutes. For example, the OSA may access medical records kept by HCPF in order to ensure that Medicaid eligibility determinations are being made properly. The OSA cannot effectively evaluate eligibility without information that specifically identifies benefit recipients. The only information accessed by the OSA is that information already kept by other agencies – the OSA does not access information through direct requests of patients or their physicians.

Breach Procedures

In the event of a breach, including if the OSA receives personal medical information in an unsecure way from an agency, the OSA Information Security Policy directs that the breach be reported immediately to a supervisor. From there, the breach will be handled through destruction of the insecure information and notification of the proper parties. Instances of breach are very infrequent and have consisted solely of the loss of data that is encrypted.

University of Colorado (CU)

Privacy Statutes and Regulations

The controlling statutes and regulations for CU in regard to privacy are federal and state statutes and regulations, including HIPAA, FERPA, the ADA, and the FMLA.

Policies and Procedures

CU has extensive policies to ensure protection of personal data. CU ensures that only the minimum data necessary is accessed or requested. CU is a hybrid entity. The health plan, Wardenburg Health Center (on the Boulder campus), Health Circle clinic and the Anschutz Medical Campus are all considered health care components under HIPAA, and are fully compliant with that statute. Any department, which is not a covered entity and retains personal health information, as authorized by another federal statute, treats the information as highly confidential, and ensures its protection through the most stringent procedures CU employs (e.g. encryption).

If not authorized by federal or state law, individual consent is required for access to personal health information. Anyone with access to this information is fully trained to ensure compliance with privacy laws and regulations. Each health care component has their own HIPAA Privacy and Security Officer, undergoes regular audits by the Office of Information Security, and may occasionally be reviewed by Office of Internal Audits. Any data used outside of the health care components without a Business Associate Agreement is deidentified.

Uses

CU accesses personal health information for a variety of reasons. Among these are processing ADA reasonable accommodation requests for employees and students, claims and other data through the CU's self-funded health plan, medical malpractice claims from the Anschutz Medical Campus, worker's compensation claims, and information required to process financial aid, housing, admissions, and study abroad programs. All uses are consistent with federal and state law. If a health care component requires data analysis by a third party (e.g. an audit), Business Associate Agreements are put in place.

Breach Procedures

CU has a system-wide incident response procedure, including a system-wide data breach analysis team.

Other Comments

Additional regulations for access to personal health information would prove very burdensome and would be very difficult for CU to administer. HIPAA already addresses the health data used by the University. Requiring a separate, more heightened policy in Colorado appears to be redundant and would be difficult due to CU's national and international reach.

APPENDIX D
Sample of Colorado Laws Concerning Health Information Privacy

Title & Enforcing Agency	Citation & Description
False Medicaid Claims - Liability for Certain Acts (HCPF)	C.R.S § 25.5-4-305
Disease Reporting and Investigation (CDPHE)	C.R.S. § 25-1-122 (allowing access to medical records for tracking disease) 6 CCR 1009-1 (including HIV/AIDS and sexually transmitted infections) C.R.S. § 25-4-1401 et seq. 6 CCR 1009-9
Tuberculosis (CDPHE)	C.R.S. § 25-4-501 et seq.
Newborn metabolic screening (CDPHE)	§ §25-4-1004(b), C.R.S. and 6 CCR 1009-25-4-1007
	CRCSN, §25-1.5-102(1)(r), C.R.S. and 6 CCR 1009-7
Vital Statistics (birth, death, marriage, etc.) (CDPHE)	§ 25-2-101 et seq., C.R.S. and 5 CCR 1006-1
Cancer reporting (CDPHE)	§ §25-1.5-102(1)(q), C.R.S. and 6 CCR 1009-3
Immunization reporting (CDPHE)	§ §25-4-2401 et seq, C.R.S
Health facility inspections (CDPHE)	§ § 25-1-124, C.R.S. and multiple CCRs, general licensure found at 6 CCR 1011-1, Ch. 2
Radiation (CDPHE)	§ 6 CCR 1007-1, Sections 4.6, 4.18 and 4.56
Trauma (CDPHE)	§ Designation, § 25-3.5-704(2)(d), C.R.S. and 6 CCR 1015-4, Ch. 3
	§ Registry, § 25-3.5-704(2)(f), C.R.S. and 6 CCR 1015-4, Ch. 1
EMS (CDPHE)	§ Provider investigations, §25-3.5-205(4), C.R.S. and 6 CCR 1015-3, Ch. 1
	§ EMS data collection, § 25-3.5-501, C.R.S. and 6 CCR 1015-3, Ch. 3
	§ Statewide Continuous Quality Improvement (EMTS), § 25-3.5-704(2)(h), C.R.S.
Refugee Program (CDPHE)	United States Refugee Act of 1980 (Public Law 96-212)
Blood/lead screening (CDPHE)	Environmental and Chronic Diseases 6 CCR 1009-7
CRCCP (CDPHE)	CRCCP - 1) 45 CFR §164.512(b)(1)(i) public health activities – permitted disclosures
Family Planning (CDPHE)	Title X
Newborn hearing screening (CDPHE)	§ 25-4-1004.7, C.R.S. and 6 CCR 1009-7
Old Age Pension Dental Assistance (CDPHE)	§25-21-104(2)(a)(II)(d) and §25-21-106, C.R.S.

Department of Regulatory Agencies (DORA)	"The board shall conduct investigations, hold hearings and take evidence in all-matters relating to the exercise and performance of the powers and duties of the boards (C.R.S. 12-42.5-106 (1)(i)(I), 12-36-118) (C.R.S. 12-42.5-131,120, and 106)(C.R.S. 13-90-107(1)(d)(III)(C), and (2).
State Board of Nursing (DORA)	§ Nurses Practice Act - C.R.S.12-38-111(1)(a); (3); 12-38-112(1)(a); (3); 12-38-112.5(4), (8); 12-38-116.5(4)(c)(III)(A); (7); (8)(a), (b), (c), & (d); (13)(a); 12-38-117(1)(c),(f), (h), (i), & (j); and 12-38-131(5). Nurse Aide Practice Act – C.R.S. 12-38.1-111(1)(i), (j), & (k); 12-38.1-113(1); (1)(p); (2)(a); (3); and 12-38.1-113(5). Psychiatric Technician Practice Act – C.R.S. 12-42-113(1)(i) & (j); 12-42-115.3 - which refers back to 12-38-116.5 (as listed above).
Medical Board (DORA)	§ 13-90-107(1)(d)(III)(C), 12-36-104((1)(b),(3), 12-36-118, 12-35.5-101 et seq. C.R.S.; Board Policy 10-16; 42 CFR Part 2 (Health Oversight Activities PHI can be disclosed for activities related to oversight of the health care system. Examples of health oversight activities include audits; investigations, inspections; and licensure and disciplinary actions.)
Mental Health Board (DORA)	§ Sections 12-43-221 (1)(b)(III), 12-43-221, 12-43-224, C.R.S.
ATs (DORA)	§ C.R.S. sections 12-29.7-109, 110 (grounds for discipline, and mental or physical examinations of registrants, respectively.)
SLPs (DORA)	§ See sections 13-90-107(1)(d)(III)(C), 12-43.7-102,12-43.7-111, 42 CFR Part 2 (Health Oversight Activities PHI can be disclosed for activities related to oversight of the health care system. Examples of health oversight activities include audits; investigations, inspections; and licensure and disciplinary actions.)
State Auditor's Office	Statutorily obligated through Colorado State Statute 23.1072A, to investigate operations of agencies within the state government.
Department of RevenuC-Department of Motor Vehicles	Titles and Registration- Persons with Disabilities C.R.S. 42-3-204; 42-4-1208; Driver's Privacy Protection Act of 1994; 42-1-206 1.B Licenses- C.R.S. Fit to Drive 42-2-111; 42-2-116 Authority to place restrictions

APPENDIX E
Sample Business Associate Agreement

The following agreement template is publicly available through the University of Colorado Anschutz Medical Campus's website.[15]

HIPAA BUSINESS ASSOCIATE ADDENDUM

This Business Associate Addendum ("Addendum") is a part of the Agreement dated _____ between the Regents of the University of Colorado, a body corporate, for and on behalf of the University of Colorado Denver, _____ ("University") and _____ ("Contractor"), Agreement number _____. For purposes of this Addendum, the University is referred to as "Covered Entity" or "CE" and the Contractor is referred to as "Associate". Unless the context clearly requires a distinction between the Agreement document and this Addendum, all references herein to "the Agreement" or "this Agreement" include this Addendum.

RECITALS

A. CE wishes to disclose certain information to Associate pursuant to the terms of the Agreement, some of which may constitute Protected Health Information ("PHI") (defined below).

B. CE and Associate intend to protect the privacy and provide for the security of PHI disclosed to Associate pursuant to this Agreement in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA") and regulations promulgated thereunder by the U.S. Department of Health and Human Services (the "HIPAA Regulations") and other applicable laws, as amended.

C. As part of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) including all pertinent regulations (45 CFR Parts 160 and 164) issued by the U.S. Department of Health and Human Services as either have been amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act (the "HITECH" Act), as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5), the Privacy Rule (defined below) requires CE to enter into a contract containing specific requirements with Associate prior to the disclosure of PHI.

The parties agree as follows:

1. Definitions.

a. Except as otherwise defined herein, capitalized terms in this Addendum shall have the definitions set forth in the HIPAA Privacy Rule at 45 CFR Parts 160 and 164, as amended ("Privacy Rule"). In the event of any conflict between the mandatory provisions of the Privacy Rule and the provisions of this Agreement, the Privacy Rule shall control. Where the provisions of this Agreement differ from those mandated by the Privacy Rule, but are nonetheless permitted by the Privacy Rule, the provisions of this Agreement shall control.

[15] Available, along with other HIPAA policies and procedures for the University of Colorado, at: http://www.ucdenver.edu/academics/research/AboutUs/regcomp/hipaa/Pages/policies-forms.aspx (Accessed October 10, 2014)

b. "Protected Health Information" or "PHI" means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 CFR Section 164.501.

c. "Protected Information" shall mean PHI provided by CE to Associate or created or received by Associate on CE's behalf.

2. Obligations of Associate.

a. Permitted Uses. Associate shall not use Protected Information except for the purpose of performing Associate's obligations under this Agreement and as permitted under this Addendum. Further, Associate shall not use Protected Information in any manner that would constitute a violation of the Privacy Rule if so used by CE, except that Associate may use Protected Information: (i) for the proper management and administration of Associate; (ii) to carry out the legal responsibilities of Associate; or (iii) for Data Aggregation purposes for the Health Care Operations of CE, if applicable. Additional provisions, if any, governing permitted uses of Protected Information are set forth in Attachment A to this Addendum. Associate accepts full responsibility for any penalties incurred as a result of Associate's breach of the Privacy Rule.

b. Permitted Disclosures. Associate shall not disclose Protected Information in any manner that would constitute a violation of the Privacy Rule if disclosed by CE, except that Associate may disclose Protected Information: (i) in a manner permitted pursuant to this Agreement; (ii) for the proper management and administration of Associate; (iii) as required by law; (iv) for Data Aggregation purposes for the Health Care Operations of CE, if applicable; or (v) to report violations of law to appropriate federal or state authorities, consistent with 45 CFR Section 502(j)(1). To the extent that Associate discloses Protected Information to a third party, Associate must obtain, prior to making any such disclosure: (i) reasonable assurances from such third party that such Protected Information will be held confidential as provided pursuant to this Addendum and only disclosed as required by law or for the purposes for which it was disclosed to such third party; and (ii) an agreement from such third party to immediately notify Associate of any breaches of confidentiality of the Protected Information, to the extent it has obtained knowledge of such breach. Additional provisions, if any, governing permitted disclosures of Protected Information are set forth in Attachment A.

c. Appropriate Safeguards. Associate shall implement appropriate safeguards as are necessary to prevent the use or disclosure of Protected Information other than as permitted by this Agreement. Associate shall comply with the requirements of the Security Rules, 164.308, 164.310, 164.312, and 164.316. Associate shall maintain a comprehensive written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Associate's operations and the nature and scope of its activities.

d. Reporting of Improper Use or Disclosure. Associate shall report in writing to CE Representative, identified in Section 15. b, any use or disclosure of Protected Information in violation of the Privacy Rule within three (3) days of becoming aware of such use or disclosure.

e. Associate's Agents. If Associate uses one or more subcontractors or agents to provide services under the Agreement, and such subcontractors or agents receive or have access to Protected

Information, each subcontractor or agent shall sign a Business Associate Agreement with Associate containing substantially the same provisions as this Addendum and further identifying CE as a third party beneficiary with rights of enforcement from such subcontractors or agents in the event of any violation of such subcontractor or agent agreement. Associate's subcontractors or agents may not use Protected Information in a manner not permitted by the Business Associate Agreement. Associate shall implement and maintain sanctions against agents and subcontractors that violate such restrictions and conditions and shall mitigate the effects of any such violation.

f. Access to Protected Information. Associate shall make Protected Information maintained by Associate or its agents or subcontractors in Designated Record Sets available to CE for inspection and copying within five (5) days of a request by CE to enable CE to fulfill its obligations to permit individual access to PHI under the Privacy Rule, including, but not limited to, 45 CFR Section 164.524.

g. Amendment of PHI. Within five (5) days of receipt of a request from CE for an amendment of Protected Information or a record about an individual contained in a Designated Record Set, Associate or its agents or subcontractors shall make such Protected Information available to CE for amendment and incorporate any such amendment to enable CE to fulfill its obligations with respect to requests by individuals to amend their PHI under the Privacy Rule, including, but not limited to, 45 CFR Section 164.526. If any individual requests an amendment of Protected Information directly from Associate or its agents or subcontractors, Associate must notify CE in writing within five (5) days of receipt of the request and make such amendments to the extent required by the Privacy Rule.

h. Accounting Rights. Within ten (10) days of notice by CE of a request for an accounting of disclosures of Protected Information, Associate and its agents or subcontractors shall make available to CE the information required to provide an accounting of disclosures to enable CE to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR Section 164.528. As set forth in, and as limited by, 45 CFR Section 164.528, Associate shall not provide an accounting to CE of disclosures: (i) to carry out treatment, payment or health care operations, as set forth in 45 CFR Section 164.506; (ii) to individuals of Protected Information about them as set forth in 45 CFR Section 164.502; (iii) pursuant to an authorization as provided in 45 CFR Section 164.508; (iv) to persons involved in the individual's care or other notification purposes as set forth in 45 CFR Section 164.510; (v) for national security or intelligence purposes as set forth in 45 CFR Section 164.512(k)(2); or (vi) to correctional institutions or law enforcement officials as set forth in 45 CFR Section 164.512(k)(5); (vii) incident to a use or disclosure otherwise permitted by the Privacy Rule; (viii) as part of a limited data set under 45 C.F.R. Section 164.514(e); or (ix) disclosures prior to April 14, 2003. Associate agrees to implement a process that allows for an accounting to be collected and maintained by Associate and its agents or subcontractors for at least six (6) years prior to the request, but not before the compliance date of the Privacy Rule. At a minimum, such information shall include: (i) the date of disclosure; (ii) the name of the entity or person who received Protected Information and, if known, the address of the entity or person; (iii) a brief description of Protected Information disclosed; and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's authorization, or a copy of the written request for disclosure. In the event that the request for an accounting is delivered directly to Associate or its agents or subcontractors, Associate shall within five (5) business days of the receipt of the request forward it to CE in writing. It shall be CE's responsibility to prepare and deliver any such accounting requested. Associate shall not disclose any Protected Information except as set forth in Section 2(b) of this Addendum.

i. Governmental Access to Records. Associate shall make its internal practices, books and records relating to the use and disclosure of Protected Information available to the Secretary of the U.S. Department of Health and Human Services (the "Secretary"), in a time and manner designated by the Secretary, for purposes of determining CE's compliance with the Privacy Rule. Associate shall provide to

CE a copy of any Protected Information that Associate provides to the Secretary concurrently with providing such Protected Information to the Secretary.

j. Minimum Necessary. Associate (and its agents or subcontractors) shall only request, use and disclose the minimum amount of Protected Information necessary to accomplish the purpose of the request, use or disclosure, in accordance with the Minimum Necessary requirements of the Privacy Rule including, but not limited to 45 C.F.R. Sections 164.502(b) and 164.514(d).

k. Data Ownership. Associate acknowledges that Associate has no ownership rights with respect to the Protected Information.

l. Retention of Protected Information. Notwithstanding Section 4(d) of this Addendum, Associate and its subcontractors or agents shall retain all Protected Information throughout the term of this Agreement and shall continue to maintain the information required under Section 2(h) of this Addendum for a period of six (6) years after termination of the Agreement.

m. Associate's Insurance. In addition to any insurance requirements in the Agreement, Associate shall maintain casualty and liability insurance to cover loss of PHI data and claims based upon alleged violations of privacy rights through improper use or disclosure of PHI. All such policies shall meet or exceed the minimum insurance requirements of the Agreement (e.g., occurrence basis, combined single dollar limits, annual aggregate dollar limits, additional insured status and notice of cancellation).

n. Notification of Breach. During the term of this Agreement, Associate shall promptly notify CE of any suspected or actual breach of security, intrusion or unauthorized use or disclosure of PHI and/or any actual or suspected use or disclosure of data in violation of any applicable federal or state laws or regulations Such notice shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed to have been accessed, acquired, or disclosed during the breach. Associate shall take (i) prompt corrective action to cure any such deficiencies and (ii) any action pertaining to such unauthorized disclosure required by applicable federal and state laws and regulations.

o. Audits, Inspection and Enforcement. Upon receipt of a written request by CE, Associate and its agents or subcontractors shall allow CE to conduct a reasonable inspection of the facilities, systems, books, records, agreements, policies and procedures relating to the use or disclosure of Protected Information pursuant to this Addendum for the purpose of determining whether Associate has complied with this Addendum; provided, however, that: (i) Associate and CE shall mutually agree in advance upon the scope, timing and location of such an inspection; (ii) CE shall protect the confidentiality of all confidential and proprietary information of Associate to which CE has access during the course of such inspection; and (iii) CE shall execute a nondisclosure agreement, upon terms mutually agreed upon by the parties, if requested by Associate. The fact that CE inspects, or fails to inspect, or has the right to inspect, Associate's facilities, systems, books, records, agreements, policies and procedures does not relieve Associate of its responsibility to comply with this Addendum, nor does CE's (i) failure to detect or (ii) detection, but failure to notify Associate or require Associate's remediation of any unsatisfactory practices, constitute acceptance of such practice or a waiver of CE's enforcement rights under the Agreement.

p. Safeguards During Transmission. Associate shall be responsible for using appropriate safeguards to maintain and ensure the confidentiality, privacy and security of Protected Information transmitted to CE pursuant to the Agreement, in accordance with the standards and requirements of the Privacy Rule, until such Protected Information is received by CE, and in accordance with any specifications set forth in Attachment A.

q. Restrictions and Confidential Communications. Within ten (10) business days of notice by CE of a restriction upon uses or disclosures or request for confidential communications pursuant to 45 C.F.R. 164.522, Associate will restrict the use or disclosure of an individual's Protected Information, provided Associate has agreed to such a restriction. Associate will not respond directly to an individual's requests to restrict the use or disclosure of Protected Information or to send all communication of Protect Information to an alternate address. Associate will refer such requests to the CE so that the CE can coordinate and prepare a timely response to the requesting individual and provide direction to Associate.

3. Obligations of CE.

a. Safeguards During Transmission. CE shall be responsible for using appropriate safeguards to maintain and ensure the confidentiality, privacy and security of PHI transmitted to Associate pursuant to this Agreement, in accordance with the standards and requirements of the Privacy Rule, until such PHI is received by Associate, and in accordance with any specifications set forth in any attachment to this Agreement.

b. Notice of Changes. CE shall provide Associate with a copy of its notice of privacy practices produced in accordance with 45 CFR Section 164.520, as well as any subsequent changes or limitation(s) to such notice, to the extent such changes or limitations may effect Associate's use or disclosure of Protected Information. CE shall provide Associate with any changes in, or revocation of, permission to use or disclose Protected Information, to the extent it may affect Associate's permitted or required uses or disclosures. To the extent that it may affect Associate's permitted use or disclosure of PHI, CE shall notify Associate of any restriction on the use or disclosure of Protected Information that CE has agreed to in accordance with 45 CFR Section 164.522. CE may effectuate any and all such notices of non-private information via posting on CE's web site.

4. Termination.

a. Material Breach. In addition to any other provisions in the Agreement regarding breach, a breach by Associate of any provision of this Addendum, as determined by CE, shall constitute a material breach of this Agreement and shall provide grounds for immediate termination of this Agreement by CE pursuant to the provisions of the Agreement covering termination for cause, if any. If the Agreement contains no express provisions regarding termination for cause, the following terms and conditions shall apply:

(1) Default. If Associate refuses or fails to timely perform any of the provisions of this Agreement, CE may notify Associate in writing of the non-performance, and if not promptly corrected within the time specified, CE may terminate this Agreement. Associate shall continue performance of this Agreement to the extent it is not terminated.

(2) Associate's Duties. Notwithstanding termination of this Agreement, and subject to any directions from CE, Associate shall take timely, reasonable and necessary action to protect and preserve property in the possession of Associate in which CE has an interest.

(3) Compensation. Payment for completed supplies delivered and accepted by CE shall be at the Agreement price.

(4) Erroneous Termination for Default. If after such termination it is determined, for any reason, that Associate was not in default, or that Associate's action/inaction was excusable, such termination shall be treated as a termination for convenience, and the rights and obligations of the parties

shall be the same as if this Agreement had been terminated for convenience, to the extent described in this Agreement.

b. Reasonable Steps to Cure Breach. If CE knows of a pattern of activity or practice of Associate that constitutes a material breach or violation of the Associate's obligations under the provisions of this Addendum or another arrangement and does not terminate this Agreement pursuant to Section 4(a), then CE shall take reasonable steps to cure such breach or end such violation, as applicable. If CE's efforts to cure such breach or end such violation are unsuccessful, CE shall either (i) terminate the Agreement, if feasible or (ii) if termination of this Agreement is not feasible, CE shall report Associate's breach or violation to the Secretary of the Department of Health and Human Services.

c. Judicial or Administrative Proceedings. Either party may terminate the Agreement, effective immediately, if (i) the other party is found guilty or pleads nolo contendere in a criminal proceeding for a violation of HIPAA, the HIPAA Regulations or other security or privacy laws or (ii) a finding or stipulation that the other party has violated any standard or requirement of HIPAA, the HIPAA Regulations or other security or privacy laws is made in any administrative or civil proceeding in which the party has been joined.

d. Effect of Termination.

(1) Except as provided in paragraph (2) of this subsection, upon termination of this Agreement, for any reason, Associate shall return or destroy all Protected Information that Associate or its agents or subcontractors still maintain in any form, and shall retain no copies of such Protected Information. If Associate elects to destroy the PHI, Associate shall certify in writing to CE that such PHI has been destroyed.

(2) If Associate believes that returning or destroying the Protected Information is not feasible, Associate shall promptly provide CE notice of the conditions making return or destruction infeasible. Upon mutual agreement of CE and Associate that return or destruction of Protected Information is infeasible, Associate shall continue to extend the protections of Sections 2(a), 2(b), 2(c), 2(d) and 2(e) of this Addendum to such information, and shall limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible.

5. Injunctive Relief. CE shall have the right to injunctive and other equitable and legal relief against Associate or any of its subcontractors or agents in the event of any use or disclosure of Protected Information in violation of this Agreement or applicable law.

6. No Waiver of Immunity. No term or condition of this Agreement shall be construed or interpreted as a waiver, express or implied, of any of the immunities, rights, benefits, protection, or other provisions of the Colorado Governmental Immunity Act, CRS 24-10-101 *et seq.* or the Federal Tort Claims Act, 28 U.S.C. 2671 *et seq.* as applicable, as now in effect or hereafter amended.

7. Limitation of Liability. Any limitation of Associate's liability in the Agreement shall be inapplicable to the terms and conditions of this Addendum.

8. Disclaimer. CE makes no warranty or representation that compliance by Associate with this Agreement, HIPAA or the HIPAA Regulations will be adequate or satisfactory for Associate's own purposes. Associate is solely responsible for all decisions made by Associate regarding the safeguarding of PHI.

9. Certification. To the extent that CE determines an examination is necessary in order to comply with CE's legal obligations pursuant to HIPAA relating to certification of its security practices, CE or its

authorized agents or contractors, may, at CE's expense, examine Associate's facilities, systems, procedures and records as may be necessary for such agents or contractors to certify to CE the extent to which Associate's security safeguards comply with HIPAA, the HIPAA Regulations or this Addendum.

10. Amendment.

a. Amendment to Comply with Law. The parties acknowledge that state and federal laws relating to data security and privacy are rapidly evolving and that amendment of this Addendum may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the Privacy Rule and other applicable laws relating to the security or privacy of PHI. The parties understand and agree that CE must receive satisfactory written assurance from Associate that Associate will adequately safeguard all Protected Information. Upon the request of either party, the other party agrees to promptly enter into negotiations concerning the terms of an amendment to this Addendum embodying written assurances consistent with the standards and requirements of HIPAA, the Privacy Rule or other applicable laws. CE may terminate this Agreement upon thirty (30) days written notice in the event (i) Associate does not promptly enter into negotiations to amend this Agreement when requested by CE pursuant to this Section or (ii) Associate does not enter into an amendment to this Agreement providing assurances regarding the safeguarding of PHI that CE, in its sole discretion, deems sufficient to satisfy the standards and requirements of HIPAA and the Privacy Rule.

b. Amendment of Attachment A. Attachment A may be modified or amended by mutual agreement of the parties in writing from time to time without formal amendment of this Addendum.

11. Assistance in Litigation or Administrative Proceedings. Associate shall make itself, and any subcontractors, employees or agents assisting Associate in the performance of its obligations under the Agreement, available to CE, at no cost to CE, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CE, its directors, officers or employees based upon a claimed violation of HIPAA, the Privacy Rule or other laws relating to security and privacy or PHI, except where Associate or its subcontractor, employee or agent is a named adverse party.

12. No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than CE, Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

13. Interpretation and Order of Precedence. The provisions of this Addendum shall prevail over any provisions in the Agreement that may conflict or appear inconsistent with any provision in this Addendum. Together, the Agreement and this Addendum shall be interpreted as broadly as necessary to implement and comply with HIPAA and the Privacy Rule. The parties agree that any ambiguity in this Agreement shall be resolved in favor of a meaning that complies and is consistent with HIPAA and the Privacy Rule. This Agreement supersedes and replaces any previous separately executed HIPAA addendum between the parties.

14. Survival of Certain Agreement Terms. Notwithstanding anything herein to the contrary, Associate's obligations under Section 4(d) ("Effect of Termination") and Section 12 ("No Third Party Beneficiaries") shall survive termination of this Agreement and shall be enforceable by CE as provided herein in the event of such failure to perform or comply by the Associate. This Addendum shall remain in effect during the term of the Contract including any extensions.

15. Representatives and Notice.

a. Representatives. For the purpose of the Agreement, the individuals identified elsewhere in this Agreement shall be the representatives of the respective parties. If no representatives are identified in the Agreement, the individuals listed below are hereby designated as the parties' respective representatives for purposes of this Agreement. Either party may from time to time designate in writing new or substitute representatives.

b. Notices. All required notices shall be in writing and shall be hand delivered or given by certified or registered mail to the representatives at the addresses set forth below.

University/Covered Entity Representative:

Title:	Privacy Officer
Department and Division:	Office of Regulatory Compliance
Address:	Mail Stop F497 13001 East 17th Place Aurora, Colorado 80045

Contractor/Business Associate Representative:

Name:	_____
Title:	_____
Department and Division:	_____
Address:	_____