ALAMEDA COUNTY DEPARTMENT OF BEHAVIORAL HEALTH CARE SERVICES COMPLIANCE AND INTEGRATED ETHICS PLAN

***Revised: December* 2016**

TABLE OF CONTENTS

ALAMEDA COUNTY BEHAVIORAL HEALTH CARE CODE OF CONDUCT

- All employees, vendors, contractors and their employees are responsible for reviewing and understanding the ACBHCS Compliance and Integrated Ethics Plan.

- All employees, vendors, contractors and their employees SHALL agree to abide by and not violate any of the Department's Policies and Procedures or Code of Ethics.

- All employees, vendors, contractors and their employees SHALL conduct themselves and treat others with integrity, honesty, courtesy, fairness, and in a respectful manner.

- No employee, vendor, contractor or their employees SHALL engage in activities that violate any federal, state or local laws, regulations, rules, policy or procedures.

- All employees, vendors, contractors and their employees SHALL promptly report any activities that they believe violate any policy or procedure, this Code of Conduct or any federal, state, or local law, regulation, rule, policy or procedure. Such reporting will be in accordance with the Rules and Regulations for reporting set forth in policy

- Any employee, vendor, contractor or their employee with questions regarding any policy or procedure SHALL seek clarification and consultation immediately with their supervisor, Executive Staff, or designee.

ALAMEDA COUNTY
DEPARTMENT OF BEHAVIORAL HEALTH CARE SERVICES
COMPLIANCE AND INTEGRATED ETHICS PLAN

PURPOSE

The Alameda County Department of Behavioral Health Care Services (ACBHCS) has adopted this Compliance and Integrated Ethics Plan (CIEP) to ensure clarity of responsibility for actions and to provide standards by which employees and contractors of the Department shall conduct themselves. The Plan provides guidance designed to ensure proper and professional behavior in order to protect and promote organization-wide integrity. The CIEP is also a means of expressing departmental standards and expectations to its employees, and its vendors, contractors, their employees, and other individuals or entities providing services on behalf of the Alameda County Department of Behavioral Health Care Services.

The CIEP is the Department's design to comply with applicable Federal, State and local standards through the establishment of an effective compliance program that is targeted to reduce the risk of unlawful or improper conduct and to support the highest quality of data submission, as evidenced by accuracy, reliability, timeliness, and validity. This is done with the knowledge that these efforts shall eliminate fraud, abuse, and waste from the service delivery system.

INTRODUCTION

The ACBHCS, its employees, vendors, contractors, and their employees are dedicated to providing quality care to clients served. ACBHCS demands ethical standards and uses its best efforts to comply with both the letter and spirit of all federal, state, and local laws, regulations, rules, guidelines, ordinances and funding sources. To ensure that best efforts are taken to comply with all laws, the ACBHCS has developed a Compliance and Integrated Ethics Plan and Program (CIEP).

The CIEP is intended to ensure that ACBHCS, including all its employees and its vendors, contractors and their employees, do not violate laws that apply to the business of delivering health care services, and that they have sufficient familiarity with those laws which are relevant to their specific job performance. The CIEP also sets forth the objectives and requirements regarding compliance and expectations for the Department's employees, and its vendors, contractors and their employees

To ensure the effectiveness of the CIEP:

- ✓ ACBHCS will dedicate the necessary resources to develop an effective Compliance and Integrated Ethics Program (CIEP) designed to prevent and detect violations of Federal or State law in the conduct of ACBHCS's operations;
- ✓ The CIEP shall meet or exceed the elements of an effective program by:

- Establishing compliance standards and procedures reasonably capable of eliminating the prospect of wrongful conduct;
- Maintaining a Compliance Officer on staff with responsibility to monitor the compliance hotline and address complaints as appropriate.
- Taking steps to communicate effectively the compliance standards and procedures to all employees, vendors, contractors and their employees by providing mandatory training sessions *and/or* the distribution and dissemination of relevant publications;
- Taking steps to achieve compliance by utilizing monitoring and auditing systems, and by publicizing a reporting system whereby employees and agents can report perceived wrongful conduct by others within the organization without fear of retribution;
- Taking steps to respond appropriately to confirmed non-compliance issues and to prevent recurrence.

ACBHCS shall distribute the CIEP, including a **Code of Ethics**, to all employees. All employees of the ACBHCS shall be required to certify, in writing, that they have received, read, understand and will abide by the requirements set out in the CIEP and the supporting policies and procedures. ACBHCS shall obtain, as part of the employee annual evaluation, a written certification from each employee that he/she has received, read, understands and shall abide by the ACBHCS Code of Ethics Policy. Any action taken in violation of the CIEP or outside the scope of employment could subject the individual to serious sanctions, including termination of employment and criminal prosecution. *(Code of Ethics – Attachment A)*

Employees shall receive, initially and annually thereafter, on-site education regarding the CIEP, and all relevant Laws addressed therein. Any employee who has questions or concerns about anything discussed in the plan should contact their supervisor.

RESOURCES FOR GUIDANCE AND REPORTING VIOLATIONS

To obtain guidance on an ethics or compliance issue or to report a suspected violation, individuals may select from several options. ACBHCS encourages the resolution of issues at the lowest level whenever possible. It is an expected good practice, when individuals are comfortable with it and think it appropriate under the circumstances, to raise concerns first with the person in question. If this is uncomfortable or inappropriate, another option is to discuss the situation with the immediate supervisor or another member of management. The individual is always free to use the whistleblower hotline at 1-844-729-7055 and may report issues anonymously.

ACBHCS shall make every effort to maintain, within the limits of the law, the confidentiality of any individual who reports possible misconduct. There shall be no retribution or discipline for anyone who reports a possible violation in good faith. Any employee who deliberately makes a

false accusation with the purpose of harming or retaliating against another employee shall be subject to discipline.

PERSONAL OBLIGATION TO REPORT

ACBHCS is committed to ethical and legal conduct that is compliant with all relevant laws and regulations and to correct wrongdoing wherever it may occur in the department. Each employee has an individual responsibility for reporting any activity by employees, vendors, contractors, or their employees that appears to violate applicable laws, rules, regulations, policies and procedures.

INTERNAL INVESTIGATION OF REPORTS

ACBHCS is committed to investigate all reported concerns promptly and confidentially to the extent possible. ACBHCS shall coordinate any findings from the investigations and immediately recommend corrective action or changes. ACBHCS expects all employees to cooperate fully with investigation efforts

CORRECTIVE ACTION

Where an internal investigation substantiates a reported violation, it is the policy of ACBHCS to initiate corrective action including, as appropriate:

- Making prompt restitution of any overpayment amounts,
- Notifying the appropriate governmental agency,
- Instituting whatever disciplinary action is necessary and appropriate,
- Implementing systematic changes to prevent a similar violation from reoccurring

DISCIPLINE

All violators shall be subject to disciplinary action in accordance with Alameda County Human Resources Rules and Regulations

ACKNOWLEDGEMENT PROCESS

ACBHCS shall distribute the CIEP including the Code of Ethics Policy, to all employees. All employees of the ACBHCS shall be required to certify, in writing, that they have received, read, understand and shall abide by the requirements set out in the CIEP and the overall programs. At implementation and with all new employees the Department shall be required to provide thorough training and to certify in writing the employee has received, read, understands and will abide by the CIEP. Annually, at the time of the employee performance appraisal, ACBHCS shall obtain written certification that he/she has received, read, understands and will abide by the CIEP. Any action taken in violation of the CIEP or outside the scope of employment could subject the individual to serious sanctions, including termination of employment and criminal prosecution. ACBHCS requires all new employees to sign the acknowledgement of the Code of Ethics Policy

DEFINITIONS OF FRAUD AND ABUSE

The Center for Medicare and Medicaid Services (CMMS) has issued the following definitions as they relate to fraud and abuse:

- **FRAUD:** knowingly and willfully executing, or attempting to execute, a scheme or artifice to defraud any health care benefit program or to obtain, by means of false or fraudulent pretenses, representations, or promises, any of the money or property owned by, or under the custody or control of, any health care benefit program.

- **ABUSE:** actions which directly or indirectly, result in unnecessary costs to the health care benefit program, improper payment or payment for services which fail to meet professionally recognized standards of care, or that are medically unnecessary. Abuse involves payment for items or services when there is no legal entitlement to that payment and the provider has not knowingly and/or intentionally misrepresented facts to obtain payment

EMPLOYEES AND CONTRACTORS

All employees, vendors, contractors and employees of vendors and contractors must adhere to these policies and procedures:

- ✓ All contracts with vendors, contractors and providers shall include language that requires the contractor to adhere to CIEP policies and procedures. It is the policy of the ACBHCS to annually monitor all contracts and written agreements for compliance and contractual requirements including adherence to its compliance policies and procedures.

- ✓ ACBHCS or its vendors or contractors shall not employ a person who has had a previous criminal conviction related to healthcare or has been excluded from participation in federal healthcare programs.

- ✓ ACBHCS shall not enter into any contractual agreement with any entity or company that has been convicted of criminal offenses related to healthcare that has been excluded or made otherwise ineligible to participate in federal healthcare programs.

- ✓ It is the policy of ACBHCS to terminate the employment of any employee, or agreement with any vendor or contractor, or any agreement with any person or organization that is convicted of any criminal offense related to healthcare or that is excluded or otherwise made ineligible to participate in any federal healthcare program.

- ✓ ACBHCS shall provide training to all employees related to accepted policies and procedures as well as any training necessary to provide staff with the knowledge and skills to comply with accepted policies and procedures. Such training will include, but will not be limited to: orientation to relevant policies and procedures, provider eligibility, coding, documentation standards, and maintenance of records.

- ✓ In addition to the above listed training, all supervisors shall be responsible for periodic employee orientation, including initial orientation of new employees and additional orientation on relevant policies and procedures as well as ongoing monitoring of compliance.

- ✓ Managers and supervisors shall be subject to discipline for failure to instruct subordinates and/or failure to detect noncompliance where reasonable diligence on the part of the manager or supervisor would have led to knowledge and awareness of the particular violation and provided the ACBHCS with the opportunity to take corrective action

GENERAL COMPLIANCE TRAINING

ACBHCS shall train all employees by requiring attendance at mandatory training sessions. The Department shall maintain a record of the curriculum and a log of attendees. Training shall be scheduled for new employees upon hire and completed within their first 30 work days and on an annual basis for all employees following their orientation. The training format is to be developed by the Compliance Officer. Additionally the ACBHCS shall provide area specific compliance training to vendors and contract providers. A certificate shall be awarded upon completion of training.

Deliver annual training in the following areas[1]:

- Compliance and Integrated Ethics Plan (CIEP)
- Behavioral Health Care Services Department Code of Ethics
- Security Policies and Procedures
- Privacy Policies and Procedures
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- 42 CFR, Part 2
- Annual Employee Acknowledgment Pursuant to the Deficit Reduction Act of 2005 and subsequent amendments
- Fraud, Waste, and Abuse

[1] Delivery may be via document, email, supervisor, website, or other means.

THE COMPLIANCE AND INTEGRATED ETHICS PROGRAM

OVERSIGHT

ACBHCS and the Compliance Officer shall monitor overall compliance with federal, state and local laws, regulations, rules, policies and procedures. A compliance officer with senior management designation shall be assigned to oversee the overall compliance plan and activities including the department-wide implementation of accepted policies, procedures and training. A Compliance Committee shall be established with representation from major areas of the department to assist the Compliance Officer. The Compliance Committee shall include the following members.

- Compliance Officer
- Behavioral Health Director
- Behavioral Health Deputy Director
- Quality Improvement and/or Quality Assurance Personnel
- Behavioral Health Care Services Employee Training Department
- Behavioral Health Care Services Fiscal Manager
- Behavioral Health Care Services IT Director; and
- Consumer and Family Member Representation as designated by Behavioral Health Care Services

Compliance Committee Duties

1. Address new and/or changing regulations and laws
2. Provide information and potential risk areas to the Compliance Committee.
3. Discuss training and ways in which annual training may be conducted/tracked.
4. Annually review and update the CIEP as needed
5. Act as liaison to Divisions with the Department
6. Operate cohesively and respectfully to fulfill the CIEP

MONITORING THE COMPLIANCE PLAN

The Compliance Officer shall be responsible for monitoring all aspects of the CIEP. To successfully monitor this plan, the Compliance Officer, along with assistance from the Compliance Committee, shall monitor the following:

- Periodic review of medical charts through the Utilization Review (UR) Team, which shall conduct an annual review of at least five percent of all charts.

- Monthly review of at least five percent of insurance claims by the Fiscal Department prior to submission to the payer;

- Annual review of a predetermined percentage of medical records with their corresponding billing;

- Review and maintenance of attendance logs related to mandated compliance trainings;

- Review of minutes from Medical Records, Managed Care, Utilization Review, Quality Improvement, Fiscal and other related staff meetings and committee to ensure ongoing compliance;

- Maintenance of a log of compliance activities, such as training, and policy and procedure changes, undertaken by ACBHCS;

- Oversight of all compliance investigations

Compliance Officer Duties

- Maintain complete records and logs of all compliance issues, reports, investigations, and outcomes

- Implement and operate the ACBHCS compliance program and provide direct oversight and supervision to the Privacy and Security Officers.

- Advise and consult with ACBHCS Executive Team on the compliance program goals, objectives, and results annually.

- Referring program or site specific issues to the System of Care Directors/Program Managers to initiate change as necessary;

- Ensure that any/all applicable State and Federal law and regulation are published to staff and CBO's.

- Provide an annual report of all compliance issues/concerns to the Behavioral Health Care Services Director

DOCUMENTATION

Documentation of services rendered to patients/clients is essential to the continuity and quality of care provided. The documentation itself is to be of such a level of quality as to ensure continuity of care with other providers, provide an accurate history of care provided and adequately support the rationale for the type of services rendered and billed. ACBHCS has documentation standards to which all service delivery staff are expected to adhere.

- The record shall include the following:
  - ✓ Medical Necessity as mandated by funding source rules and regulations
  - ✓ Relevant history
  - ✓ Findings of any diagnostic tests
  - ✓ An assessment of the patient and the diagnosis
  - ✓ Plan of Care
  - ✓ Identified client strengths
  - ✓ Progress Notes

- All services provided must be documented in the patient/client medical record at the time the service was rendered. Documentation shall include, according to the programs policies and procedures, any of the following:
  - ✓ Location that service was provided
  - ✓ Reason for contact or service
  - ✓ Identity and credentials of the person providing care
  - ✓ Date service was rendered
  - ✓ Progress and/or response to treatment
  - ✓ Plan developed

- Documentation must be accurate, complete and legible

- Current diagnosis that includes documentation supporting the diagnosis

- Past and present diagnoses are clearly documented along with the rationale for the diagnosis when appropriate

- Rationale/documentation supporting any test or ancillary services ordered

ACBHCS shall ensure that all records are maintained for the period of time required by federal, state and local laws and regulations or contractual requirements

CLAIM DEVELOPMENT AND SUBMISSION

Service providers, such as ACBHCS and its contracted entities, who furnish items and services, and submit claims for items or services provided to patients covered by an insurance plan, including Medicare, Medi-Cal, and private insurance, are subject to statutory and regulatory obligations. These obligations include providing items and services only when medically necessary and which are of a quality that meets professionally recognized standards of care.

The Federal Civil Monetary Penalty Law prohibits any person or organization from presenting or causing to be presented to the Federal Government any claim for medical item or service that the claimant knows, or should know, was not provided as claimed. This shall include any person who engages in any pattern or practice of presenting a claim for an item or service that is based on a code that the person knows or should know will result in a greater payment than would the correct code that the person knows or should know is applicable to the item or service actually provided, i.e., "up coding."

Additionally, the Federal False Claims Act prohibits the submission of false and fraudulent claims to the Federal Government if the person or agency submitting the claim knows or should know the claim is false or fraudulent.

Federal laws similarly prohibit fraudulent billing, including statutes governing false statements and representations, wire and mail fraud, and criminal conspiracy. These statutes apply to private insurance carriers as well as federally funded health care programs such as Medicare and Medi-Cal. In addition, California has laws prohibiting false or fraudulent submission of claims to the Medi-Cal program and to private insurance companies

ALAMEDA COUNTY BEHAVIORAL HEALTH CARE SERVICES – GENERAL POLICIES

ACBHCS requires that all staff, contract providers and vendors shall only bill for the correct patient, within the usual and legally accepted standards. In addition to more specific policies and procedures established by ACBHCS, it has developed the following ***general policies,*** which reflect and reinforce current Federal and State statutes and regulations regarding the proper development and submission of claims to third party payers:

- No claim shall be submitted to any payer or patient by ACBHCS, or others acting on its behalf, for items or services not provided or rendered.

- No claim shall be submitted to any payer or patient for services that are not medically necessary, that is, services that are not warranted by the patient's current documented medical condition.

- All items and services shall be reviewed by the service provider prior to billing to ensure only those accurately coded and documented items or services will be billed to payers and patients.

- Claims shall only be submitted when appropriate documentation supports the claims, and only when such documentation is maintained and available for audit and review.

- Records and notes relied upon as the basis for claim submissions shall be appropriately organized in legible form for audit and review.

- The items or services reported on claims shall be based on the medical record and other documentation, and the documentation necessary for accurate code assignment will be available to appropriate staff.

- Any form of "up-coding", i.e., using a billing code that provides for a higher payment rate than the billing code that accurately reflects the product or service furnished to the patient/client, is strictly prohibited.

- Duplicate billing, i.e. submitting more than one claim for the same service or submitting the same claim more than once, is prohibited.

- Any form of "unbundling", submitting bills in a piecemeal or fragmented fashion for products or services which are required to be billed together, for the purpose of increasing reimbursement, is strictly prohibited. (Federal payment plans require certain services that are typically considered to be integral parts of one procedure to be billed in one lump, or "bundled" sum).

- No claim shall be submitted to any payer for more than the actual cost of a service, item or drug.

- Under no circumstances shall compensation for ACBHCS employees responsible for performing, supervising, or monitoring coding or billing, provide any financial incentive of any nature, to improperly code claims.

- No claim shall be submitted to any payer or patient using an incorrect or inappropriate provider number.

CODING AND BILLING

Coding and billing are areas of particularly sensitive regulatory compliance. In most situations, staff of ACBHCS, and its contract providers, who provide direct service, determine and document/report the proper code for the procedure/service provided. Thus, it is imperative that staff providing direct service have an accurate understanding of the definitions and descriptions of procedure/service codes used and their relation to services being provided. ACBHCS has adopted the following policies to further promote accurate coding and billing:

- ACBHCS shall follow recognized rules and regulations for accurate coding approved by the Center for Medicare and Medicaid Services (CMMS) or other regulatory body.

- ACBHCS shall use current billing codes, including, as appropriate, those established or approved by Health Care Financing Administration (HCFA), California Behavioral Health Care Services Department of Behavioral Health Care Services, California Department of Alcohol and Drug Programs, CMMS and all other applicable government entities and payers.

- ACBHCS shall provide staff with current and up to date code manuals that have descriptive information for each procedure code that will enable staff and providers to make a determination of the appropriate codes to use when documenting/entering/ reporting a service/procedure that has been provided.

- All codes reported for claiming and billing purposes shall have supporting documentation in the patient record.

- In preparing the appropriate form(s), ACBHCS employees and/or its contracted providers shall:

    - ✓ Link a single, most appropriate diagnosis with the corresponding service code;
    - ✓ Use procedure codes and modifiers (i.e. intense/rehab/half day) appropriately where necessary; and
    - ✓ Provide insurance plans, including Medicare, with all appropriate information about a patient's other insurance coverage.

- Billing personnel shall regularly examine denied claims to identify billing accuracy issues and changes in reimbursement policies and procedures.

- Performance and compliance with billing policies of ACBHCS by billing personnel shall be regularly monitored. The appropriate supervisor (s) shall provide regular feedback regarding performance to each individual billing employee.

- ACBHCS staff shall be advised of the mechanisms for ACBHCS employees to express their concerns, regarding the accurate coding and billing practices. Staff will be advised that any concerns about billing and coding may be discussed with their supervisor. ACBHCS policy assures no retribution for expressing such concerns. Billing and coding staff shall also be asked to sign an acknowledgement of their understanding of the reporting process for concerns/complaints regarding billing accuracy.

- Meetings of all billing staff will be conducted on a regular basis to discuss regulatory updates and directives, denied claims, periodic review, and audit results. Records of those in attendance at such meetings shall be maintained by ACBHCS.

- In the event that billing inaccuracies are discovered through any means, the inaccuracies shall be reported to the appropriate supervisor and an action plan shall be developed and implemented to correct the inaccuracies and prevent further discrepancies.

ANONYMOUS REPORTING AND NONRETALIATION POLICY

It is the responsibility of all ACBHCS employees, vendors, contract providers and their employees to comply with all laws and regulations, and to ensure that others do as well. Employees who are aware of or suspect noncompliance shall report it to their supervisors, the Compliance Officer, any member of the Compliance Committee, or may call the whistleblower hotline at 1-844-729-7055. An employee, who is aware of instances of noncompliance and who does not report such action may be subject to disciplinary action. Employees uncertain about whether conduct constitutes noncompliance should contact their supervisor, the Compliance Officer or any member of the Compliance Committee.

It is the policy of the ACBHCS that all employees be treated with respect, dignity and fairness. Discrimination, harassment or abuse of any kind is prohibited and subject to disciplinary action and/or immediate dismissal. Employees are encouraged to utilize the existing grievance process or problem resolution process established within the department whenever possible.

ACBHCS employees, vendors, contract providers, and their employees concerned about retaliation may make anonymous reports to the Compliance Officer, any member of the Compliance Committee, or through the Whistleblower Hotline. Written reports may be sent and every attempt shall be made to preserve the confidentiality of the reports of noncompliance. However, when it is necessary to disclose information, only the facts/information vital to the investigation shall be disclosed.

It is the policy of ACBHCS that no person shall retaliate, in any form, against a person who reports in good faith, an act or suspected act of noncompliance, regardless of the outcome of the report. Any person who is found to have retaliated for such a report in violation of this policy shall be subject to disciplinary action

INVESTIGATING NON-COMPLIANCE

Every report of non-compliance shall be investigated under the direction of the Compliance Officer and/or his/her designee. All investigations of noncompliance shall be concluded within sixty (60) working days of the date of notification.

The investigation may include interviewing employees and/or reviewing documentation. All ACBHCS employees must cooperate with such investigations.

Once the investigation is complete, the Compliance Officer shall submit a written report and make a verbal report to the ACBHCS Compliance Committee. The written report shall contain a summary of the initial report, the findings of the investigation and a recommendation for minimizing future risk. Any determination of a need for corrective or disciplinary action shall be the decision of the Behavioral Health Care Services Director or designee.

SELF REPORTING AND CREDIT BALANCES

If an investigation determines that an overpayment was made to ACBHCS, the department shall refund any excess reimbursement to the appropriate payer. Examples of overpayments, or "credit balances" occur when ACBHCS is:

- Paid twice for the same service, either by the same payer or a combination of payers;
- Paid for services that were planned, but not provided;
- Paid for services that were not a covered benefit;
- Overpaid due to an error in calculation, either by ACBHCS or the payer; or
- Paid for services that were considered "inclusive" of the per diem rate.

In instances where ACBHCS exercised reasonable care in billing for an appropriate service, the department may not be liable for refunding the payment. Reasonable care is considered to have been exercised when ACBHCS has:

- Complied with all pertinent regulations and instructional materials/manuals;
- Made full disclosure of all medical facts, and
- Had a reasonable basis for assuming that the payment was correct, or if the payment was questionable, it was immediately brought to the payer's attention.

However, it is department policy to make full disclosure of suspected overpayments, to fully document all efforts to remedy the situation, to refund the overpaid amount, and to develop and/or revise procedures to assure that the error is avoided in the future

ANTI-KICKBACK LAWS, INDUCEMENTS, AND SELF-REFERRALS

The federal government has enacted laws designed to prohibit staff, vendors, contract providers and their employees from accepting or providing monetary incentives related to the provision of service, billing, and referrals. Violation of these laws is a felony and may result in fines, imprisonment, and/or exclusion from participation in federal and state healthcare programs. Pursuant to the laws listed below, ACBHCS has established the following Rules and Regulations and policies:

- ACBHCS employees, vendors, contract providers and their employees are prohibited from knowingly and willfully paying, offering, asking for or receiving any money or other benefit, directly or indirectly, from third parties in connection with items or services billed to government funded programs.

- ACBHCS employees, vendors, contract providers and their employees are prohibited from knowingly and willfully offering anything of monetary value to a physician or outside referral source to induce referrals of governmental or private health care beneficiaries.

- ACBHCS employees, vendors, contract providers and their employees are prohibited from providing remuneration for referrals which may affect the quality of patient/client care by encouraging physicians to order services or items based on profit rather than the patient/client's best medical interests.

- ACBHCS employees, contract providers, and vendors shall not sign blank records or certification forms, or provide patient identification numbers which shall be used by another entity to obtain payment.

- ACBHCS employees, contract providers, and vendors shall not refer or accept referrals from entities in which they, or immediate family members, have a financial relationship, such as a partnership or affiliation (Stark Law).

- All contract arrangements for professional services must be in writing, have a predetermined term, and specify the compensation. Compensation shall be based on a "fair market value" basis.

- ACBHCS employees, vendors, contract providers and their employees shall not offer inducements to patients such as waiving insurance co-payments and deductibles without a determination of the patient's financial ability to pay. Routine waiver of deductibles and co-payments is considered fraudulent and is prohibited. Deductibles and co-payments may be waived on an individual basis only for financial hardship that would prevent the client from receiving necessary behavioral health services and only according to established procedures.

- ACBHCS shall not offer physicians or any staff member a percentage share of any reduction in the cost for patient care attributable in part to the staff person's efforts (known as "gainsharing").

- ACBHCS employees, contract providers, and vendors shall make every effort to collect patient insurance, co- payments, deductibles and liabilities. No account shall be "written-off" without appropriate prior approval from the Behavioral Health Care Services Director or his designee

Applicable Laws, Regulations, Statutes, and Policies

Code of Ethics
Anti-Kickback Statute
Anti-trust Laws
Civil Monetary Penalty Law
Emergency Medical Treatment and Active Labor Act (EMTALA)
Federal False Claims Act
Health and Human Services Freedom of Information Act (FOIA)
Health and Insurance Portability and Accountability Act (HIPAA)
Stark Laws I and II
Title XIX – Medicaid
Title XVIII – Medicare

MEDICAL NECESSITY

No payment may be made for a service or product that is not reasonable and necessary for the diagnosis and treatment of a behavioral health disorder. Billing for services that are unnecessary and excessive is considered fraudulent. While it is recognized that medical necessity in behavioral healthcare is often difficult to define, the following general Rules and Regulations are to be considered in determining whether a service is medically necessary:

- ✓ The service is consistent with the diagnosis or symptoms of the illness (condition) for which the patient/client is being treated.
- ✓ The service is consistent with the generally accepted professional behavioral health standards for the profession.
- ✓ The service is provided at a level that is most appropriate for the safe and effective treatment of the patient/client.
- ✓ The service is provided by a professional or other provider qualified by both training and licensure (or other appropriate certification or credentialing process) to provide the service.

For Short-Doyle Medi-Cal billed services, the following additional standards for medical necessity must be met:

1. The patient/client has an "included" diagnosis for the particular service being billed;
2. The patient/client has one of the following impairments as a result of a mental disorder:
   A significant impairment in an important area of life functioning, and/or
   A probability of significant deterioration in an important area of life functioning, or
   A probability that a child will not progress developmentally as individually appropriate (child is defined as a person under age 21);
3. And must meet each of the following:
   Focus of intervention is to address the condition in 2 above;
   The intervention is expected to significantly diminish the impairment;
   To prevent significant deterioration in an important area of life functioning;
   To allow the child to progress developmentally as individually appropriate; and
   The condition is not responsive to physical health care based treatment

RECORDS

ACBHCS shall retain records related to compliance activities for evidence that the organization has exercised due diligence in its compliance efforts. Records shall be retained for legally required time periods or seven years, whichever comes last, before being destroyed. Such records shall include but not be limited to:

- ✓ Clinical ("Medical") records of individual patient/client
- ✓ Training records: Attendance records, outlines, topics, handouts
- ✓ Results of internal audits including plans of correction

"INCIDENT TO" PHYSICIAN SERVICES

In respect to the Federally funded Medicare program, services provided by non-physician staff are only billable in certain instances, and only when provided under the direct supervision of specific certified licensed staff. For ACBHCS services and items, only a Psychiatrist or Licensed Clinical Psychologist, certified by the appropriate payer source, may employ other psychological practitioners (Licensed Clinical Social Workers) directly under their supervision to provide services. These services are referred to as "incident to." ACBHCS employees holding Marriage and Family Therapist (MFT) or Registered Nurse (RN) licenses are not eligible to provide "incident to" services. ACBHCS employees shall adhere to the following "incident to" requirements, which provide that: (reference: MCM B3 2150, MCM 2050.1)

I. Staff providing "incident to" services shall be certified by Medicare and receive a UPIN number prior to provision of services.

II. The service supplied shall be under the direct supervision of the practitioner (Psychiatrist/Psychologist) under whose license Medicare and other payer sources are billed. The practitioner is the "incident to" supervisor and is referred to as the "licentiate."

III. The "incident to" practitioner's (LCSW) service will be an integral, although incidental, part of the professional services supplied by the licentiate.

IV. The Psychiatrist/Psychologist shall be physically present in the vicinity of the rendering service providers and immediately available to provide assistance and direction throughout the time the "incident to" practitioner is supplying the service. Availability of the Psychiatrist/Psychologist by telephone or at a distant location elsewhere in the institution is insufficient to qualify as direct "incident to" supervision.

V. The "incident to" LCSW must be a County employee or Contractor. The employer may be the licentiate, group practice of the licentiate, or employer of the licentiate; or a controlled leased employee of one of these arrangements; as defined under the common law test. Association and supervision alone do not meet requirements.

VI. The Psychiatrist/Psychologist actively participates in the management and treatment of the patient, with appropriate frequency. This requires periodic patient visits by the Psychiatrist/Psychologist. Appropriate and timely interaction with the "incident to" LCSW is also required.

VII. The Psychiatrist/Psychologist shall identify each date of service supervised. The Psychiatrist/Psychologist must date and sign one of the following:

- ✓ The chart note for each date of services supervised, or
- ✓ A periodic supervisory session with the "incident to" LCSW that references each date of service supplied.

VIII. Medication management services using CPT coders are not sufficient to meet the test for supervision of an "incident to" LCSW. More specific supervision of the psychotherapy is required.

IX. The "incident to" LCSW related service must be within the scope of the practitioner's license, and within the scope of the Psychiatrist/Psychologist's license.

X. Verification of the "incident to" LCSW related employment and State license covering the dates of service is maintained. State licensed psychotherapy interns may work "incident to" if all State and payer requirements are met and documented. The intern may only supply service in a place of service authorized by the State. The supervisor of psychotherapy can only be a M.D., D.O., or C.P. All other supervision billings will be denied.

XI. The Psychiatrist/Psychologist shall initiate the course of treatment in order to meet the direct supervision requirements. If a practitioner is not qualified to bill a government payer source directly and initiates therapy, the service must be billed with the proper modifier attached to the procedure code indicating the care is not supplied as "incident to."

DISCLOSURE TO PATIENTS

For non-emergency situations, at the time of service delivery or immediately thereafter, ACBHCS shall inform all patients of the following:

- ✓ Eligible and covered services pursuant to all applicable Federal and State Laws, regulations and individual insurance carrier plans;
- ✓ The amount of any co-payments or deductibles;
- ✓ That their private insurance carrier shall be billed first and that any amounts not deemed eligible by their insurance carrier shall become their responsibility;
- ✓ Any instances in which Medicare and/or third party payers will not be billed for eligible services and the patient's liability.

Note: In emergency situations, services shall be provided prior to any determination of financial ability.

Under the Omnibus Budget Reconciliation Act (OBRA) of 1986, ACBHCS must provide Medicare beneficiaries, at the time of service, a written statement that explains:

- ✓ The patient's right to benefits for both inpatient hospital services and outpatient services;
- ✓ Any liability the patient may have for the cost of services received;
- ✓ The patient's right to appeal denials of benefits, including the steps to initiate the process,
- ✓ The patient's right to appeal for the cost of services that have been denied if the denial is upheld upon appeal.

- ✓ A statement that the patient's liability for the cost of non-covered services begins the day following the date of receipt of their continued stay notice of non-coverage (in-patient services only).

ACBHCS shall inform all patients of their right to report non-compliance with this policy. Such information shall be provided in writing.

All notices shall be issued in English and the recognized Medi-Cal threshold languages.

POTENTIAL AREAS OF RISK

It is essential for ACBHCS to be cognizant of potential areas of risk related to reimbursement and licensure. Noncompliance in these areas places the department in jeopardy of loss of revenues and sanctions. A loss or restriction related to licensure may also jeopardize ACBHCS's ability to provide quality services to its clients/participants and the community. Strict adherence to this policy will minimize possible exposure to risk of noncompliance. Areas of particular concern include:

- ✓ Financial arrangements with outside entities to whom the department may refer patients who are governmental healthcare beneficiaries;
- ✓ Joint ventures with entities supplying goods or services to the department or its patients;
- ✓ Consulting contracts or medical directorship;
- ✓ Soliciting, accepting or offering any gift or gratuity to or from those who may benefit from a referral of governmental healthcare business;
- ✓ Contracting with a third party for billing services;
- ✓ "Incident to" billing;
- ✓ Up coding and "unbundling" services;
- ✓ Billing for services or goods that are not reasonable and necessary;
- ✓ Failure to provide "Advanced Beneficiary Notices" to patients when services or goods are not eligible for federal reimbursement;
- ✓ Billing for non-covered services as if they were covered;
- ✓ Submitting false cost reports; and
- ✓ *Waivers of coinsurance and deductibles which were not routinely offered, advertised to the general public, made in good-faith based on financial need or hardship, or approved in advance by the Psychiatric Facility Manager, Assistant Director, or Director*

Alameda County Department of Behavioral Health Care Services
Compliance and Integrated Ethics Plan
DECEMBER 2016

ATTACHMENTS

Attachment A

CODE OF ETHICS

POLICY STATEMENT

In accordance with Alameda County Behavioral Health Care Services (ACBHCS) standards, ethical conduct should be evidenced throughout the activities of all personnel of the organization including both management, direct service staff*, County operated providers, independent providers and the contractual providers which incorporate the Behavioral Health Plan's provider network. The ethical conduct should be seen in communications with the consumers served, payers, and the community. It is expected that ethical conduct is demonstrated in how clinicians involve the clients and their families in the treatment process and outcomes, and how all persons that are part of or representative of the ACBHCS' organization communicate with funding sources and other regulatory agencies.

POLICY

Alameda County Behavioral Health Care services adheres to written codes of ethical conduct related to its organizational staff, provider network, governance authority, business and financial practices, marketing activities, treatment of consumers and community members.

ACBHCS has defined ethical codes and conduct for its organization by addressing primary philosophical beliefs, principles and values that are considered exceptional in promoting the kind of relationships and subsequent environment whereby services can be provided in an exemplary manner. Ethical conduct is expected at all levels of the organization, not only in provision of services and the correctness in billing for those services, but in everyday activities from regular business plans, decision-making processes, meetings and policy development.

ACBHCS' ethical conduct policy is in accordance with the several licensing boards and professional organizations that address its standards of professional conduct.

Orientation and educational programs are provided to employees and contractual providers, in addition, to the written Ethical Conduct Policy and Ethical Conduct Standards within contracts.

ACBHCS resolves allegations of violations of its codes of ethical conduct by referring them to the Credentials Committee when it involves the BHP's provider network and to the appropriate administrative operations office for county-operated and contracted services.

NOTE: All references to staff refer to management, direct services and contracted staff.

CORE VALUES

The following are the core values that act as a guide for actions of staff and providers, treatment of consumers served, and business/financial practices and marketing:

RESPECT FOR EACH OTHER - Thoughtful consideration of others including clients and their family members, colleagues, supervisors, staff we supervise, community members, other agency staff, regulatory agencies and governing boards.

PROFESSIONAL PRACTICES - A commitment to professional practice that is competent, objective, and provided with integrity.

HONESTY - The value of honesty cannot be compromised. It is expected that employees and contractors in their association with consumers, agencies and other staffs will be honest without being harmful.

TRUST - A non-judgmental position on issues that do not directly pertain to you or your ability to conduct business provides a supportive environment. When indicated during a time of need, a supportive position for others is taken.

NON-DISCRIMINATORY MANNER - A commitment to society offering opportunities to all its members in a just and non-discriminatory manner.

CLIENT PRIVACY - A commitment and obligation to monitor the privacy of both current and former clients, whether living or deceased, and to Monitor the confidentiality of material that has been transmitted to you in your professional role.

POLICY ON COMPLIANCE CODE OF CONDUCT AND RELATIONSHIPS

- Staff/contractor will adhere to Medi-Cal and Medicare standards and procedures as required by federal and state regulatory agencies.
- Staff/contractor will not knowingly and willingly falsify medical records by erroneously documenting assessment findings, diagnostic formulations, or the amount of time and/or type of services rendered to consumers. Improper alterations to documentation are included, as it constitutes medical records falsification.
- Staff/contractor is responsible to ensure the integrity and confidentiality of client and medical records information, to ensure compliance from employees they supervise, and to investigate and report any hazards or threats to the security or integrity of client information to appropriate staff within your organization.

Standard

- Staff/contractors do not exploit professional relationships sexually, financially or for any other professional and/or personal advantage. This standard of conduct is maintained toward all who may be professionally associated with you.

Sexual Relationships

- Sexual activity or involvement with the staff member's/contractors current or former ACBHCS service system client is prohibited.
- Sexual harassment of any ACBHCS client is prohibited. This includes sexual solicitation, physical advances, or verbal or nonverbal conduct that is sexual in nature.

Personal Relationships

- Staff may provide to, receive from, or exchange articles of value with their clients only within the provisions of an ACBHCS or contract agency-sanctioned program (e.g. art show and sale, food or clothing collection project. etc.)
- When clients receive money or articles of value through an agency-sanctioned project, the client will not be informed of the individual donor's identity.

Staff/Contractor(s) are prohibited from the Following:

- Promising or entering into any personal, professional, financial or other relationship with a client that is not a part of their assigned duties within the program at which they are employed.
- Employing or using the services of their own current or former client for personal gain, except within the bounds of an agency-sanctioned project.
- Borrowing or accepting money or articles of value from clients, except within the bounds of an agency-sanctioned project, e.g. approved culturally sensitive activity.
- Loaning or giving personal funds or articles of value to clients, except within the bounds of an agency-sanctioned project, e.g. provision of funds for clients when reimbursement of these funds by the agency will occur or approved culturally sensitive activity.
- Using the relative position of power afforded by their staff position to influence clients in any way not directly relevant to the client's treatment or service goals.
- Living with their current or former ACBHCS clients.
- Staff should refrain from religious proselytizing to clients and/or employees.
- Providing massage to clients, except within the bounds of a formal job description and any applicable State licensure.
- Providing any form of treatment not sanctioned by the employing program's formally recognized program design or the service definitions and procedures of the ACBHCS.

POLICY ON SELF-PROMOTION AND REFERRAL

Standard

- Clear, appropriate professional standards are set to prevent engagement in dual or multiple relationships in which there is any risk of professional judgment being compromised, or of the client being harassed or exploited.

- Staff may not refer ACBHCS clients to their own private practices, businesses, or any other service in which a staff member has a personal or financial interest.
- Staff will present themselves accurately and not misrepresent their roles, scope of practice or professional status in the course of their work with clients and the community.
- Staff may not receive self-referred ACBHCS clients or ACBHCS clients referred by a third party into their private practices except as follows:
    - Under certain exceptional circumstances, a client who initiates a request for a private professional relationship with an ACBHCS service system staff member may be permitted to enter into such a relationship if no other adequate public or private resource is available to meet the client's needs. Supervisory approval is required. Such approvals must be documented and the total number of such private self-referrals must be reported by the Supervisor at the end of each calendar year to the Quality Assurance Administrator.
    - Under certain circumstances in order to meet client's needs, ACCESS may refer to a private practitioner who also is employed by ACBHCS. This is done with the approval of the Director of ACCESS.
- In order to protect the client from undue influence and the Agency from potential conflicts of interest, the staff member receiving the private referral must agree to the guidelines listed in the Self-Disclosure section below...
- Staff who have continuing private professional relationships with ACBHCS clients that were entered into either before the effective date of this policy or that were entered into before the client became an ACBHCS client, must comply with the provisions of IV Pre-Existing Professional Relationships section below.

SELF DISCLOSURE OF PRE-EXISTING PROFESSIONAL RELATIONSHIPS

It is the policy of this agency to comply with the Alameda County Behavioral Health Care Services "Policy on Multiple Relationships and Staff Self-Promotion." In recognition of the rights of clients to exercise choice in therapeutic relationships under appropriate circumstances, the following disclosure information will be communicated to the supervisor based on the following:

1. A staff member is entering into a private professional relationship with a client because no other adequate public or private resource is available to meet the client's needs or;
2. A staff member had a pre-existing private professional relationship with a client prior to client receiving services from ACBHCS or;
3. A staff member had a pre-existing private professional relationship with a client prior to the effective date of this policy.

When a staff person agrees to enter into a private professional relationship with a client, the following has occurred:

- The clinician has encouraged this client to return, and appropriately terminate, any existing client/therapist relationships before entering into one with him/her.
- The clinician has determined that no other public sector, private or nonprofit agency resource is available to adequately meet the client's needs.
- The clinician has not solicited this client's business in any way, nor used his/her position in this agency to advertise his/her services as an independent practitioner.
- The clinician has explicitly stated to the supervisor that the decision to enter such relationship will not affect the client's County services in any manner, except that he/she will exclude him/herself from any decisions in the future that affect the client's care within the County system, since this could represent conflict of interest

I ACKNOWLEDGE AND UNDERSTAND THE AFOREMENTIONED CODE OF ETHICS AND SHALL COMPLY WITH ANY AND ALL PROVISIONS AND REQUIREMENTS. AS AN EMPLOYEE OF ACBHCS I ATTEST THAT I HAVE RECEIVED A COPY OF THIS CODE OF ETHICS WITH MY SIGNATURE BELOW:

Employee Name and Signature

DATE

ATTACHMENT B

42 U.S. Code § 1395dd - Examination and treatment for emergency medical conditions and women in labor (EMTALA)

(a) Medical screening requirement

In the case of a hospital that has a hospital emergency department, if any individual (whether or not eligible for benefits under this subchapter) comes to the emergency department and a request is made on the individual's behalf for examination or treatment for a medical condition, the hospital must provide for an appropriate medical screening examination within the capability of the hospital's emergency department, including ancillary services routinely available to the emergency department, to determine whether or not an emergency medical condition (within the meaning of subsection (e)(1) of this section) exists.

(b) Necessary stabilizing treatment for emergency medical conditions and labor

(1) In general If any individual (whether or not eligible for benefits under this subchapter) comes to a hospital and the hospital determines that the individual has an emergency medical condition, the hospital must provide either—

(A) within the staff and facilities available at the hospital, for such further medical examination and such treatment as may be required to stabilize the medical condition, or

(B) For transfer of the individual to another medical facility in accordance with subsection (c) of this section.

(2) Refusal to consent to treatment

A hospital is deemed to meet the requirement of paragraph (1) (A) with respect to an individual if the hospital offers the individual the further medical examination and treatment described in that paragraph and informs the individual (or a person acting on the individual's behalf) of the risks and benefits to the individual of such examination and treatment, but the individual (or a person acting on the individual's behalf) refuses to consent to the examination and treatment. The hospital shall take all reasonable steps to secure the individuals (or person's) written informed consent to refuse such examination and treatment.

(3) Refusal to consent to transfer

A hospital is deemed to meet the requirement of paragraph (1) with respect to an individual if the hospital offers to transfer the individual to another medical facility in accordance with subsection (c) of this section and informs the individual (or a person acting on the individual's behalf) of the risks and benefits to the individual of such transfer, but the individual (or a person acting on the

individual's behalf) refuses to consent to the transfer. The hospital shall take all reasonable steps to secure the individuals (or person's) written informed consent to refuse such transfer.

(c) Restricting transfers until individual stabilized

(1) Rule If an individual at a hospital has an emergency medical condition which has not been stabilized (within the meaning of subsection (e) (3) (B) of this section), the hospital may not transfer the individual unless—

(A)

(I) the individual (or a legally responsible person acting on the individual's behalf) after being informed of the hospital's obligations under this section and of the risk of transfer, in writing requests transfer to another medical facility,

(ii) a physician (within the meaning of section 1395x(r)(1) of this title) has signed a certification that [1] based upon the information available at the time of transfer, the medical benefits reasonably expected from the provision of appropriate medical treatment at another medical facility outweigh the increased risks to the individual and, in the case of labor, to the unborn child from effecting the transfer, or

(iii) if a physician is not physically present in the emergency department at the time an individual is transferred, a qualified medical person (as defined by the Secretary in regulations) has signed a certification described in clause (ii) after a physician (as defined in section 1395x(r)(1) of this title), in consultation with the person, has made the determination described in such clause, and subsequently countersigns the certification; and

(B) The transfer is an appropriate transfer (within the meaning of paragraph (2)) to that facility.

A certification described in clause (ii) or (iii) of subparagraph (A) shall include a summary of the risks and benefits upon which the certification is based.

(2) Appropriate transfer an appropriate transfer to a medical facility is a transfer—

(A) In which the transferring hospital provides the medical treatment within its capacity which minimizes the risks to the individual's health and, in the case of a woman in labor, the health of the unborn child;

(B) In which the receiving facility—

(I) has available space and qualified personnel for the treatment of the individual, and

(ii) Has agreed to accept transfer of the individual and to provide appropriate medical treatment;

(C) in which the transferring hospital sends to the receiving facility all medical records (or copies thereof), related to the emergency condition for which the individual has presented, available at

the time of the transfer, including records related to the individual's emergency medical condition, observations of signs or symptoms, preliminary diagnosis, treatment provided, results of any tests and the informed written consent or certification (or copy thereof) provided under paragraph (1)(A), and the name and address of any on-call physician (described in subsection (d)(1)(C) of this section) who has refused or failed to appear within a reasonable time to provide necessary stabilizing treatment;

(D) in which the transfer is effected through qualified personnel and transportation equipment, as required including the use of necessary and medically appropriate life support measures during the transfer; and

(E) Which meets such other requirements as the Secretary may find necessary in the interest of the health and safety of individuals transferred.

(d) Enforcement

(1) Civil money penalties

(A) A participating hospital that negligently violates a requirement of this section is subject to a civil money penalty of not more than $50,000 (or not more than $25,000 in the case of a hospital with less than 100 beds) for each such violation. The provisions of section 1320a–7a of this title (other than subsections (a) and (b)) shall apply to a civil money penalty under this subparagraph in the same manner as such provisions apply with respect to a penalty or proceeding under section 1320a–7a(a) of this title.

(B) Subject to subparagraph (C), any physician who is responsible for the examination, treatment, or transfer of an individual in a participating hospital, including a physician on-call for the care of such an individual, and who negligently violates a requirement of this section, including a physician who—

(I) signs a certification under subsection (c)(1)(A) of this section that the medical benefits reasonably to be expected from a transfer to another facility outweigh the risks associated with the transfer, if the physician knew or should have known that the benefits did not outweigh the risks, or

(Ii) misrepresents an individual's condition or other information, including a hospital's obligations under this section,

Is subject to a civil money penalty of not more than $50,000 for each such violation and, if the violation is gross and flagrant or is repeated, to exclusion from participation in this subchapter and State health care programs. The provisions of section 1320a–7a of this title (other than the first and second sentences of subsection (a) and subsection (b)) shall apply to a civil money penalty and exclusion under this subparagraph in the same manner as such provisions apply with respect to a penalty, exclusion, or proceeding under section 1320a–7a(a) of this title.

(C) If, after an initial examination, a physician determines that the individual requires the services of a physician listed by the hospital on its list of on-call physicians (required to be maintained under section 1395cc(a)(1)(I) of this title) and notifies the on-call physician and the on-call physician fails or refuses to appear within a reasonable period of time, and the physician orders the transfer of the individual because the physician determines that without the services of the on-call physician the benefits of transfer outweigh the risks of transfer, the physician authorizing the transfer shall not be subject to a penalty under subparagraph (B). However, the previous sentence shall not apply to the hospital or to the on-call physician who failed or refused to appear.

(2) Civil enforcement

(A) Personal harm

Any individual who suffers personal harm as a direct result of a participating hospital's violation of a requirement of this section may, in a civil action against the participating hospital, obtain those damages available for personal injury under the law of the State in which the hospital is located, and such equitable relief as is appropriate.

(B) Financial loss to other medical facility

Any medical facility that suffers a financial loss as a direct result of a participating hospital's violation of a requirement of this section may, in a civil action against the participating hospital, obtain those damages available for financial loss, under the law of the State in which the hospital is located, and such equitable relief as is appropriate.

(C) Limitations on actions

No action may be brought under this paragraph more than two years after the date of the violation with respect to which the action is brought.

(3) Consultation with quality improvement organizations

In considering allegations of violations of the requirements of this section in imposing sanctions under paragraph (1) or in terminating a hospital's participation under this subchapter, the Secretary shall request the appropriate quality improvement organization (with a contract under part B of subchapter XI of this chapter) to assess whether the individual involved had an emergency medical condition which had not been stabilized, and provide a report on its findings. Except in the case in which a delay would jeopardize the health or safety of individuals, the Secretary shall request such a review before affecting a sanction under paragraph (1) and shall provide a period of at least 60 days for such review. Except in the case in which a delay would jeopardize the health or safety of individuals, the Secretary shall also request such a review before making a compliance determination as part of the process of terminating a hospital's participation under this subchapter for violations related to the appropriateness of a medical

screening examination, stabilizing treatment, or an appropriate transfer as required by this section, and shall provide a period of 5 days for such review. The Secretary shall provide a copy of the organization's report to the hospital or physician consistent with confidentiality requirements imposed on the organization under such part B.

(4) Notice upon closing an investigation

The Secretary shall establish a procedure to notify hospitals and physicians when an investigation under this section is closed.

(e) Definitions In this section:

(1) The term "emergency medical condition" means—

(A) A medical condition manifesting itself by acute symptoms of sufficient severity (including severe pain) such that the absence of immediate medical attention could reasonably be expected to result in—

(I) placing the health of the individual (or, with respect to a pregnant woman, the health of the woman or her unborn child) in serious jeopardy,

(ii) Serious impairment to bodily functions, or

(iii) Serious dysfunction of any bodily organ or part; or

(B) With respect to a pregnant woman who is having contractions—

(I) that there is inadequate time to effect a safe transfer to another hospital before delivery, or

(ii) That transfer may pose a threat to the health or safety of the woman or the unborn child.

(2) The term "participating hospital" means a hospital that has entered into a provider agreement under section 1395cc of this title.

(3)

(A) The term "to stabilize" means, with respect to an emergency medical condition described in paragraph (1)(A), to provide such medical treatment of the condition as may be necessary to assure, within reasonable medical probability, that no material deterioration of the condition is likely to result from or occur during the transfer of the individual from a facility, or, with respect to an emergency medical condition described in paragraph (1)(B), to deliver (including the placenta).

(B) The term "stabilized" means, with respect to an emergency medical condition described in paragraph (1) (A), that no material deterioration of the condition is likely, within reasonable medical probability, to result from or occur during the transfer of the individual from a facility,

or, with respect to an emergency medical condition described in paragraph (1) (B), that the woman has delivered (including the placenta).

(4) The term "transfer" means the movement (including the discharge) of an individual outside a hospital's facilities at the direction of any person employed by (or affiliated or associated, directly or indirectly, with) the hospital, but does not include such a movement of an individual who (A) has been declared dead, or (B) leaves the facility without the permission of any such person.

(5) The term "hospital" includes a critical access hospital (as defined in section 1395x (mm) (1) of this title).

(f) Preemption

The provisions of this section do not preempt any State or local law requirement, except to the extent that the requirement directly conflicts with a requirement of this section.

(g) Nondiscrimination

A participating hospital that has specialized capabilities or facilities (such as burn units, shock-trauma units, neonatal intensive care units, or (with respect to rural areas) regional referral centers as identified by the Secretary in regulation) shall not refuse to accept an appropriate transfer of an individual who requires such specialized capabilities or facilities if the hospital has the capacity to treat the individual.

(h) No delay in examination or treatment

A participating hospital may not delay provision of an appropriate medical screening examination required under subsection (a) of this section or further medical examination and treatment required under subsection (b) of this section in order to inquire about the individual's method of payment or insurance status.

(I) Whistleblower protections

A participating hospital may not penalize or take adverse action against a qualified medical person described in subsection (c) (1) (A) (iii) of this section or a physician because the person or physician refuses to authorize the transfer of an individual with an emergency medical condition that has not been stabilized or against any hospital employee because the employee reports a violation of a requirement of this section.

(Aug. 14, 1935, Ch. 531, title XVIII, § 1867, as added Pub. L. 99–272, title IX, § 9121 (b), Apr. 7, 1986, 100 Stat. 164; amended Pub. L. 99–509, title IX, § 9307(c) (4), Oct. 21, 1986, 100 Stat. 1996; Pub. L. 99–514, title XVIII, § 1895 (b) (4), Oct. 22, 1986, 100 Stat. 2933; Pub. L. 100–203, title IV, § 4009 (a) (1), formerly § 4009 (a) (1), (2), Dec. 22, 1987, 101 Stat. 1330–56, 1330–57; Pub. L. 100–360, title IV, § 411 (b) (8) (A) (I), July 1, 1988, 102 Stat. 772; Pub. L.

100–485, title VI, § 608 (d) (18) (E), Oct. 13, 1988, 102 Stat. 2419; Pub. L. 101–239, title VI, §§ 6003 (g) (3) (D) (xiv), 6211(a)–(h), Dec. 19, 1989, 103 Stat. 2154, 2245–2248; Pub. L. 101–508, title IV, §§ 4008(b)(1)–(3)(A), 4207(a)(1)(A), (2), (3), (k)(3), formerly 4027(a)(1)(A), (2), (3), (k)(3), Nov. 5, 1990, 104 Stat. 1388–44, 1388–117, 1388–124, renumbered and amended Pub. L. 103–432, title I, § 160 (d) (4), (5) (A), Oct. 31, 1994, 108 Stat. 4444; Pub. L. 105–33, title IV, § 4201(c) (1), Aug. 5, 1997, 111 Stat. 373; Pub. L. 108–173, title VII, § 736 (a) (14), title IX, § 944 (b), (c) (1), Dec. 8, 2003, 117 Stat. 2355, 2423; Pub. L. 112–40, title II, § 261 (a) (3) (A), (E), Oct. 21, 2011, 125 Stat. 423.)

Attachment C

HEALTH AND INSURANCE PORTABILITY AND ACOUNTABILITY ACT OF 1996 (HIPAA)

Summary of the HIPAA Security Rule

This is a summary of key elements of the Security Rule including who is covered, what information is protected, and what safeguards must be in place to ensure appropriate protection of electronic protected health information. Because it is an overview of the Security Rule, it does not address every detail of each provision.

Introduction

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information.[1] To fulfill this requirement, HHS published what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule. The Privacy Rule, or *Standards for Privacy of Individually Identifiable Health Information*, establishes national standards for the protection of certain health information. The *Security Standards for the Protection of Electronic Protected Health Information* (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' "electronic protected health information" (e-PHI). Within HHS, the Office for Civil Rights (OCR) has responsibility for enforcing the Privacy and Security Rules with voluntary compliance activities and civil money penalties.

Prior to HIPAA, no generally accepted set of security standards or general requirements for protecting health information existed in the health care industry. At the same time, new technologies were evolving, and the health care industry began to move away from paper processes and rely more heavily on the use of electronic information systems to pay claims, answer eligibility questions, provide health information and conduct a host of other administrative and clinically based functions.

Today, providers are using clinical applications such as computerized physician order entry (CPOE) systems, electronic health records (EHR), and radiology, pharmacy, and laboratory systems. Health plans are providing access to claims and care management, as well as member self-service applications. While this means that the medical workforce can be more mobile and efficient (i.e., physicians can check patient records and test results from wherever they are), the rise in the adoption rate of these technologies increases the potential security risks.

A major goal of the Security Rule is to protect the privacy of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care. Given that the health care marketplace is diverse, the Security Rule is designed to be flexible and scalable

so a covered entity can implement policies, procedures, and technologies that are appropriate for the entity's particular size, organizational structure, and risks to consumers' e-PHI.

This is a summary of key elements of the Security Rule and not a complete or comprehensive guide to compliance. Entities regulated by the Privacy and Security Rules are obligated to comply with all of their applicable requirements and should not rely on this summary as a source of legal information or advice. To make it easier to review the complete requirements of the Security Rule, provisions of the Rule referenced in this summary are cited in the end notes. Visit our Security Rule section to view the entire Rule, and for additional helpful information about how the Rule applies. In the event of a conflict between this summary and the Rule, the Rule governs.

Statutory and Regulatory Background

- The *Administrative Simplification* provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) required the Secretary of HHS to publish national standards for the security of electronic protected health information (e-PHI), electronic exchange, and the privacy and security of health information.

HIPAA called on the Secretary to issue security regulations regarding measures for protecting the integrity, confidentiality, and availability of e-PHI that is held or transmitted by covered entities. HHS developed a proposed rule and released it for public comment on August 12, 1998. The Department received approximately 2,350 public comments. The final regulation, the Security Rule, was published February 20, 2003.[2] The Rule specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality, integrity, and availability of e-PHI.

The text of the final regulation can be found at 45 CFR Part 160 and Part 164, Subparts A and C.

Who is Covered by the Security Rule

- The Security Rule, like all of the Administrative Simplification rules, applies to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with a transaction for which the Secretary of HHS has adopted standards under HIPAA (the "covered entities"). For help in determining whether you are covered, use CMS's decision tool.

Read more about covered entities in the Summary of the HIPAA Privacy Rule - PDF.

Business Associates

- The HITECH Act of 2009 expanded the responsibilities of business associates under the Privacy and Security Rules. HHS is developing regulations to implement and clarify these changes.

See additional guidance on business associates.

What Information is Protected

- **Electronic Protected Health Information.** The HIPAA Privacy Rule protects the privacy of individually identifiable health information, called protected health information (PHI), as

explained in the Privacy Rule and here - PDF. The Security Rule protects a subset of information covered by the Privacy Rule, which is all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form. The Security Rule calls this information "electronic protected health information" (e-PHI).[3] The Security Rule does not apply to PHI transmitted orally or in writing.

General Rules

- The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI.

Specifically, covered entities must:

1. Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
3. Protect against reasonably anticipated, impermissible uses or disclosures; and
4. Ensure compliance by their workforce.[4]

The Security Rule defines "confidentiality" to mean that e-PHI is not available or disclosed to unauthorized persons. The Security Rule's confidentiality requirements support the Privacy Rule's prohibitions against improper uses and disclosures of PHI. The Security rule also promotes the two additional goals of maintaining the integrity and availability of e-PHI. Under the Security Rule, "integrity" means that e-PHI is not altered or destroyed in an unauthorized manner. "Availability" means that e-PHI is accessible and usable on demand by an authorized person.[5]

HHS recognizes that covered entities range from the smallest provider to the largest, multi-state health plan. Therefore the Security Rule is flexible and scalable to allow covered entities to analyze their own needs and implement solutions appropriate for their specific environments. What is appropriate for a particular covered entity will depend on the nature of the covered entity's business, as well as the covered entity's size and resources.

Therefore, when a covered entity is deciding which security measures to use, the Rule does not dictate those measures but requires the covered entity to consider:

- Its size, complexity, and capabilities,
- Its technical, hardware, and software infrastructure,
- The costs of security measures, and
- The likelihood and possible impact of potential risks to e-PHI.[6]

Covered entities must review and modify their security measures to continue protecting e-PHI in a changing environment.[7]

Risk Analysis and Management

- The Administrative Safeguards provisions in the Security Rule require covered entities to perform risk analysis as part of their security management processes. The risk analysis and management provisions of the Security Rule are addressed separately here because, by helping to determine which security measures are reasonable and appropriate for a particular covered entity, risk analysis affects the implementation of all of the safeguards contained in the Security Rule.

- A risk analysis process includes, but is not limited to, the following activities:

    - Evaluate the likelihood and impact of potential risks to e-PHI;[8]

    - Implement appropriate security measures to address the risks identified in the risk analysis;[9]

    - Document the chosen security measures and, where required, the rationale for adopting those measures;[10] and

    - Maintain continuous, reasonable, and appropriate security protections.[11]

Risk analysis should be an ongoing process, in which a covered entity regularly reviews its records to track access to e-PHI and detect security incidents,[12] periodically evaluates the effectiveness of security measures put in place,[13] and regularly reevaluates potential risks to e-PHI.[14]

Administrative Safeguards

- **Security Management Process**. As explained in the previous section, a covered entity must identify and analyze potential risks to e-PHI, and it must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.

Security Personnel. A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures.[15]

Information Access Management. Consistent with the Privacy Rule standard limiting uses and disclosures of PHI to the "minimum necessary," the Security Rule requires a covered entity to implement policies and procedures for authorizing access to e-PHI only when such access is appropriate based on the user or recipient's role (role-based access).[16]

Workforce Training and Management. A covered entity must provide for appropriate authorization and supervision of workforce members who work with e-PHI.[17] A covered entity must train all workforce members regarding its security policies and procedures,[18] and must have and apply appropriate sanctions against workforce members who violate its policies and procedures.[19]

Evaluation. A covered entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.[20]

Physical Safeguards

- **Facility Access and Control.** A covered entity must limit physical access to its facilities while ensuring that authorized access is allowed.[21]

Workstation and Device Security. A covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media.[22] A covered entity also must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of electronic protected health information (e-PHI).[23]

Technical Safeguards

- **Access Control.** A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).[24]

Audit Controls. A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.[25]

Integrity Controls. A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.[26]

Transmission Security. A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.[27]

Required and Addressable Implementation Specifications

- Covered entities are required to comply with every Security Rule "Standard." However, the Security Rule categorizes certain implementation specifications within those standards as "addressable," while others are "required." The "required" implementation specifications must be implemented. The "addressable" designation does not mean that an implementation specification is optional. However, it permits covered entities to determine whether the addressable implementation specification is reasonable and appropriate for that covered entity. If it is not, the Security Rule allows the covered entity to adopt an alternative measure that achieves the purpose of the standard, if the alternative measure is reasonable and appropriate.[28]

Organizational Requirements

- **Covered Entity Responsibilities.** If a covered entity knows of an activity or practice of the business associate that constitutes a material breach or violation of the business associate's obligation, the covered entity must take reasonable steps to cure the breach or end the violation.[29] Violations include the failure to implement safeguards that reasonably and appropriately protect e-PHI.

Business Associate Contracts. HHS is developing regulations relating to business associate obligations and business associate contracts under the HITECH Act of 2009.

Policies and Procedures and Documentation Requirements

- A covered entity must adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule. A covered entity must maintain, until six years after the later of the date of their creation or last effective date, written security policies and procedures and written records of required actions, activities or assessments.[30]

Updates. A covered entity must periodically review and update its documentation in response to environmental or organizational changes that affect the security of electronic protected health information (e-PHI).[31]

State Law

- **Preemption.** In general, State laws that are contrary to the HIPAA regulations are preempted by the federal requirements, which means that the federal requirements will apply.[32] "Contrary" means that it would be impossible for a covered entity to comply with both the State and federal requirements, or that the provision of State law is an obstacle to accomplishing the full purposes and objectives of the Administrative Simplification provisions of HIPAA.[33]

Enforcement and Penalties for Noncompliance

- **Compliance.** The Security Rule establishes a set of national standards for confidentiality, integrity and availability of e-PHI. The Department of Health and Human Services (HHS), Office for Civil Rights (OCR) is responsible for administering and enforcing these standards, in concert with its enforcement of the Privacy Rule, and may conduct complaint investigations and compliance reviews.

- Learn more about enforcement and penalties in the Privacy Rule Summary - PDF and on OCR's Enforcement Rule page.

Compliance Dates

- **Compliance Schedule.** All covered entities, except "small health plans," must have been compliant with the Security Rule by April 20, 2005. Small health plans had until April 20, 2006 to comply.

Copies of the Rule and Related Materials

- See our Combined Regulation Text of All Rules section of our site for the full suite of HIPAA Administrative Simplification Regulations and Understanding HIPAA for additional guidance material.

End Notes

[1]Pub. L. 104-191.

[2] 68 FR 8334.

[3] 45 C.F.R. § 160.103.

[4] 45 C.F.R. § 164.306(a).

[5] 45 C.F.R. § 164.304.

[6] 45 C.F.R. § 164.306(b)(2).

[7] 45 C.F.R. § 164.306(e).

[8] 45 C.F.R. § 164.306(b)(iv).

[9] 45 C.F.R. § 164.308(a)(1)(ii)(B).

[10] 45 C.F.R. § 164.306(d)(3)(ii)(B)(*1*); 45 C.F.R. § 164.316(b)(1).

[11] 45 C.F.R. § 164.306(e).

[12] 45 C.F.R. § 164.308(a)(1)(ii)(D).

[13] 45 C.F.R. § 164.306(e); 45 C.F.R. § 164.308(a)(8).

[14] 45 C.F.R. § 164.306(b)(2)(iv); 45 C.F.R. § 164.306(e).

[15] 45 C.F.R. § 164.308(a)(2).

[16] 45 C.F.R. § 164.308(a)(4)(i).

[17] 45 C.F.R. § 164.308(a)(3) & (4).

[18] 45 C.F.R. § 164.308(a)(5)(i).

[19] 45 C.F.R. § 164..308(a)(1)(ii)(C).

[20] 45 C.F.R. § 164.308(a)(8).

[21] 45 C.F.R. § 164.310(a).

[22] 45 C.F.R. §§ 164.310(b) & (c).

[23] 45 C.F.R. § 164.310(d).

[24] 45 C.F.R. § 164.312(a).

[25] 45 C.F.R. § 164.312(b).

[26] 45 C.F.R. § 164.312(c).

[27] 45 C.F.R. § 164.312(e).

[28] 45 C.F.R. § 164.306(d).

[29] 45 C.F.R. § 164.314(a)(1).

[30] 45 C.F.R. § 164.316.

[31] 45 C.F.R. § 164.316(b)(2)(iii).

[32] 45 C.F.R. § 160.203.

[33] 45 C.F.R. § 160.202.

United States Department of Health & Human Services

OCR PRIVACY BRIEF

SUMMARY OF THE HIPAA PRIVACY RULE

OCR OFFICE FOR CIVIL RIGHTS

HIPAA Compliance Assistance

SUMMARY OF
THE HIPAA PRIVACY RULE

Contents

SUMMARY OF
THE HIPAA PRIVACY RULE

Introduction	The *Standards for Privacy of Individually Identifiable Health Information* ("Privacy Rule") establishes, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services ("HHS") issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[1] The Privacy Rule standards address the use and disclosure of individuals' health information—called "protected health information" by organizations subject to the Privacy Rule — called "covered entities," as well as standards for individuals' privacy rights to understand and control how their health information is used. Within HHS, the Office for Civil Rights ("OCR") has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties. A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the health care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed. This is a summary of key elements of the Privacy Rule and not a complete or comprehensive guide to compliance. Entities regulated by the Rule are obligated to comply with all of its applicable requirements and should not rely on this summary as a source of legal information or advice. To make it easier for entities to review the complete requirements of the Rule, provisions of the Rule referenced in this summary are cited in notes at the end of this document. To view the entire Rule, and for other additional helpful information about how it applies, see the OCR website: http://www.hhs.gov/ocr/hipaa. In the event of a conflict between this summary and the Rule, the Rule governs. Links to the OCR Guidance Document are provided throughout this paper. Provisions of the Rule referenced in this summary are cited in endnotes at the end of this document. To review the entire Rule itself, and for other additional helpful information about how it applies, see the OCR website: http://www.hhs.gov/ocr/hipaa.
Statutory & Regulatory Background	The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996. Sections 261 through 264 of HIPAA require the Secretary of HHS to publicize standards for the electronic exchange, privacy and security of health information. Collectively these are known as the *Administrative Simplification* provisions. HIPAA required the Secretary to issue privacy regulations governing individually identifiable health information, if Congress did not enact privacy legislation within

	three years of the passage of HIPAA. Because Congress did not enact privacy legislation, HHS developed a proposed rule and released it for public comment on November 3, 1999. The Department received over 52,000 public comments. The final regulation, the Privacy Rule, was published December 28, 2000.[2] In March 2002, the Department proposed and released for public comment modifications to the Privacy Rule. The Department received over 11,000 comments. The final modifications were published in final form on August 14, 2002.[3] A text combining the final regulation and the modifications can be found at 45 CFR Part 160 and Part 164, Subparts A and E on the OCR website: http://www.hhs.gov/ocr/hipaa.
Who is Covered by the Privacy Rule	The Privacy Rule, as well as all the Administrative Simplification rules, apply to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA (the "covered entities"). For help in determining whether you are covered, use the decision tool at: http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp. **Health Plans.** Individual and group plans that provide or pay the cost of medical care are covered entities.[4] Health plans include health, dental, vision, and prescription drug insurers, health maintenance organizations ("HMOs"), Medicare, Medicaid, Medicare+Choice and Medicare supplement insurers, and long-term care insurers (excluding nursing home fixed-indemnity policies). Health plans also include employer-sponsored group health plans, government and church-sponsored health plans, and multi-employer health plans. There are exceptions—a group health plan with less than 50 participants that is administered solely by the employer that established and maintains the plan is not a covered entity. Two types of government-funded programs are not health plans: (1) those whose principal purpose is not providing or paying the cost of health care, such as the food stamps program; and (2) those programs whose principal activity is directly providing health care, such as a community health center,[5] or the making of grants to fund the direct provision of health care. Certain types of insurance entities are also not health plans, including entities providing only workers' compensation, automobile insurance, and property and casualty insurance. **Health Care Providers.** Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which HHS has established standards under the HIPAA Transactions Rule.[6] Using electronic technology, such as email, does not mean a health care provider is a covered entity; the transmission must be in connection with a standard transaction. The Privacy Rule covers a health care provider whether it electronically transmits these transactions directly or uses a billing service or other third party to do so on its behalf. Health care providers include all "providers of services" (e.g., institutional providers such as hospitals) and "providers of medical or health services" (e.g., non-institutional providers such as physicians, dentists and other practitioners) as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for health care.

	Health Care Clearinghouses. *Health care clearinghouses* are entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa. [7] In most instances, health care clearinghouses will receive individually identifiable health information only when they are providing these processing services to a health plan or health care provider as a business associate. In such instances, only certain provisions of the Privacy Rule are applicable to the health care clearinghouse's uses and disclosures of protected health information.[8] Health care clearinghouses include billing services, repricing companies, community health management information systems, and value-added networks and switches if these entities perform clearinghouse functions.
Business Associates	**Business Associate Defined.** In general, a business associate is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information. Business associate functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review, and billing.[9] Business associate services to a covered entity are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. However, persons or organizations are not considered business associates if their functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all. A covered entity can be the business associate of another covered entity. **Business Associate Contract.** When a covered entity uses a contractor or other non-workforce member to perform *"business associate"* services or activities, the Rule requires that the covered entity include certain protections for the information in a business associate agreement (in certain circumstances governmental entities may use alternative means to achieve the same protections). In the business associate contract, a covered entity must impose specified written safeguards on the individually identifiable health information used or disclosed by its business associates.[10] Moreover, a covered entity may not contractually authorize its business associate to make any use or disclosure of protected health information that would violate the Rule. Covered entities that have an existing written contract or agreement with business associates prior to October 15, 2002, which is not renewed or modified prior to April 14, 2003, are permitted to continue to operate under that contract until they renew the contract or April 14, 2004, whichever is first.[11] Sample business associate contract language is available on the OCR website at: http://www.hhs.gov/ocr/hipaa/contractprov.html. Also see OCR "Business Associate" Guidance.
What Information is Protected	**Protected Health Information.** The Privacy Rule protects all *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "*protected health information (PHI)*."[12]

	"Individually identifiable health information" is information, including demographic data, that relates to: • the individual's past, present or future physical or mental health or condition, • the provision of health care to the individual, or • the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.[13] Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number). The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g. **De-Identified Health Information.** There are no restrictions on the use or disclosure of de-identified health information.[14] De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two ways to de-identify information; either: 1) a formal determination by a qualified statistician; or 2) the removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.[15]
General Principle for Uses and Disclosures	**Basic Principle.** A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected heath information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information, except either: (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.[16] **Required Disclosures.** A covered entity must disclose protected health information in only two situations: (a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and (b) to HHS when it is undertaking a compliance investigation or review or enforcement action.[17] See OCR "Government Access" Guidance.
Permitted Uses and Disclosures	**Permitted Uses and Disclosures.** A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations: (1) To the Individual (unless required for access or accounting of disclosures); (2) Treatment, Payment, and Health Care Operations; (3) Opportunity to Agree or Object; (4) Incident to an otherwise permitted use and disclosure; (5) Public Interest and Benefit Activities; and

(6) Limited Data Set for the purposes of research, public health or health care operations.[18] Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

(1) To the Individual. A covered entity may disclose protected health information to the individual who is the subject of the information.

(2) Treatment, Payment, Health Care Operations. A covered entity may use and disclose protected health information for its own treatment, payment, and health care operations activities.[19] A covered entity also may disclose protected health information for the treatment activities of any health care provider, the payment activities of another covered entity and of any health care provider, or the health care operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if both covered entities have or had a relationship with the individual and the protected health information pertains to the relationship. See OCR "Treatment, Payment, Health Care Operations" Guidance.

> ***Treatment*** is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.[20]
>
> ***Payment*** encompasses activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual[21] and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual.
>
> ***Health care operations*** are any of the following activities: (a) quality assessment and improvement activities, including case management and care coordination; (b) competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (e) business planning, development, management, and administration; and (f) business management and general administrative activities of the entity, including but not limited to: de-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of the covered entity.[22]

Most uses and disclosures of psychotherapy notes for treatment, payment, and health care operations purposes require an authorization as described below.[23]

Obtaining "consent" (written permission from individuals to use and disclose their protected health information for treatment, payment, and health care operations) is optional under the Privacy Rule for all covered entities.[24] The content of a consent form, and the process for obtaining consent, are at the discretion of the covered entity electing to seek consent.

(3) Uses and Disclosures with Opportunity to Agree or Object. Informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object. Where the individual is incapacitated, in an emergency situation, or not available, covered entities generally may make such uses and disclosures, if in the exercise of their professional judgment, the use or disclosure is determined to be in the best interests of the individual.

> ***Facility Directories.*** It is a common practice in many health care facilities, such as hospitals, to maintain a directory of patient contact information. A covered health care provider may rely on an individual's informal permission to list in its facility directory the individual's name, general condition, religious affiliation, and location in the provider's facility.[25] The provider may then disclose the individual's condition and location in the facility to anyone asking for the individual by name, and also may disclose religious affiliation to clergy. Members of the clergy are not required to ask for the individual by name when inquiring about patient religious affiliation.
>
> ***For Notification and Other Purposes.*** A covered entity also may rely on an individual's informal permission to disclose to the individual's family, relatives, or friends, or to other persons whom the individual identifies, protected health information directly relevant to that person's involvement in the individual's care or payment for care. [26] This provision, for example, allows a pharmacist to dispense filled prescriptions to a person acting on behalf of the patient. Similarly, a covered entity may rely on an individual's informal permission to use or disclose protected health information for the purpose of notifying (including identifying or locating) family members, personal representatives, or others responsible for the individual's care of the individual's location, general condition, or death. In addition, protected health information may be disclosed for notification purposes to public or private entities authorized by law or charter to assist in disaster relief efforts.

(4) Incidental Use and Disclosure. The Privacy Rule does not require that every risk of an incidental use or disclosure of protected health information be eliminated. A use or disclosure of this information that occurs as a result of, or as "incident to," an otherwise permitted use or disclosure is permitted as long as the covered entity has adopted reasonable safeguards as required by the Privacy Rule, and the information being shared was limited to the "minimum necessary," as required by the Privacy Rule.[27] See OCR "Incidental Uses and Disclosures" Guidance.

(5) Public Interest and Benefit Activities. The Privacy Rule permits use and disclosure of protected health information, without an individual's authorization or permission, for 12 national priority purposes.[28] These disclosures are permitted, although not required, by the Rule in recognition of the important uses made of health information outside of the health care context. Specific conditions or limitations apply to each public interest purpose, striking the balance between the individual privacy interest and the public interest need for this information.

> ***Required by Law.*** Covered entities may use and disclose protected health information without individual authorization as *required by law* (including by

	statute, regulation, or court orders).[29] ***Public Health Activities.*** Covered entities may disclose protected health information to: (1) public health authorities authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability and to public health or other government authorities authorized to receive reports of child abuse and neglect; (2) entities subject to FDA regulation regarding FDA regulated products or activities for purposes such as adverse event reporting, tracking of products, product recalls, and post-marketing surveillance; (3) individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law; and (4) employers, regarding employees, when requested by employers, for information concerning a work-related illness or injury or workplace related medical surveillance, because such information is needed by the employer to comply with the Occupational Safety and Health Administration (OHSA), the Mine Safety and Health Administration (MHSA), or similar state law.[30] See OCR "Public Health" Guidance; CDC Public Health and HIPAA Guidance. ***Victims of Abuse, Neglect or Domestic Violence.*** In certain circumstances, covered entities may disclose protected health information to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.[31] ***Health Oversight Activities.*** Covered entities may disclose protected health information to health oversight agencies (as defined in the Rule) for purposes of legally authorized health oversight activities, such as audits and investigations necessary for oversight of the health care system and government benefit programs.[32] ***Judicial and Administrative Proceedings.*** Covered entities may disclose protected health information in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal. Such information may also be disclosed in response to a subpoena or other lawful process if certain assurances regarding notice to the individual or a protective order are provided.[33] ***Law Enforcement Purposes.*** Covered entities may disclose protected health information to law enforcement officials for law enforcement purposes under the following six circumstances, and subject to specified conditions: (1) as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests; (2) to identify or locate a suspect, fugitive, material witness, or missing person; (3) in response to a law enforcement official's request for information about a victim or suspected victim of a crime; (4) to alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death; (5) when a covered entity believes that protected health information is evidence of a crime that occurred on its premises; and (6) by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.[34]

Decedents. Covered entities may disclose protected health information to funeral directors as needed, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law.[35]

Cadaveric Organ, Eye, or Tissue Donation. Covered entities may use or disclose protected health information to facilitate the donation and transplantation of cadaveric organs, eyes, and tissue.[36]

Research. "Research" is any systematic investigation designed to develop or contribute to generalizable knowledge.[37] The Privacy Rule permits a covered entity to use and disclose protected health information for research purposes, without an individual's authorization, provided the covered entity obtains either: (1) documentation that an alteration or waiver of individuals' authorization for the use or disclosure of protected health information about them for research purposes has been approved by an Institutional Review Board or Privacy Board; (2) representations from the researcher that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purpose preparatory to research, that the researcher will not remove any protected health information from the covered entity, and that protected health information for which access is sought is necessary for the research; or (3) representations from the researcher that the use or disclosure sought is solely for research on the protected health information of decedents, that the protected health information sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is sought.[38] A covered entity also may use or disclose, without an individuals' authorization, a limited data set of protected health information for research purposes (see discussion below).[39] See OCR "Research" Guidance; NIH Protecting PHI in Research.

Serious Threat to Health or Safety. Covered entities may disclose protected health information that they believe is necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat). Covered entities may also disclose to law enforcement if the information is needed to identify or apprehend an escapee or violent criminal.[40]

Essential Government Functions. An authorization is not required to use or disclose protected health information for certain essential government functions. Such functions include: assuring proper execution of a military mission, conducting intelligence and national security activities that are authorized by law, providing protective services to the President, making medical suitability determinations for U.S. State Department employees, protecting the health and safety of inmates or employees in a correctional institution, and determining eligibility for or conducting enrollment in certain government benefit programs.[41]

	Workers' Compensation. Covered entities may disclose protected health information as authorized by, and to comply with, workers' compensation laws and other similar programs providing benefits for work-related injuries or illnesses.[42] See OCR "Workers' Compensation" Guidance. **(6) Limited Data Set.** A limited data set is protected health information from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed.[43] A limited data set may be used and disclosed for research, health care operations, and public health purposes, provided the recipient enters into a data use agreement promising specified safeguards for the protected health information within the limited data set.
Authorized Uses and Disclosures	**Authorization.** A covered entity must obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule.[44] A covered entity may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances.[45] An authorization must be written in specific terms. It may allow use and disclosure of protected health information by the covered entity seeking the authorization, or by a third party. Examples of disclosures that would require an individual's authorization include disclosures to a life insurer for coverage purposes, disclosures to an employer of the results of a pre-employment physical or lab test, or disclosures to a pharmaceutical firm for their own marketing purposes. All authorizations must be in plain language, and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data. The Privacy Rule contains transition provisions applicable to authorizations and other express legal permissions obtained prior to April 14, 2003.[46] **Psychotherapy Notes**[47]. A covered entity must obtain an individual's authorization to use or disclose psychotherapy notes with the following exceptions[48]: • The covered entity who originated the notes may use them for treatment. • A covered entity may use or disclose, without an individual's authorization, the psychotherapy notes, for its own training, and to defend itself in legal proceedings brought by the individual, for HHS to investigate or determine the covered entity's compliance with the Privacy Rules, to avert a serious and imminent threat to public health or safety, to a health oversight agency for lawful oversight of the originator of the psychotherapy notes, for the lawful activities of a coroner or medical examiner or as required by law. **Marketing.** Marketing is any communication about a product or service that encourages recipients to purchase or use the product or service.[49] The Privacy Rule carves out the following health-related activities from this definition of marketing: • Communications to describe health-related products or services, or payment

	for them, provided by or included in a benefit plan of the covered entity making the communication; • Communications about participating providers in a provider or health plan network, replacement of or enhancements to a health plan, and health-related products or services available only to a health plan's enrollees that add value to, but are not part of, the benefits plan; • Communications for treatment of the individual; and • Communications for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or care settings to the individual. Marketing also is an arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information, in exchange for direct or indirect remuneration, for the other entity to communicate about its own products or services encouraging the use or purchase of those products or services. A covered entity must obtain an authorization to use or disclose protected health information for marketing, except for face-to-face marketing communications between a covered entity and an individual, and for a covered entity's provision of promotional gifts of nominal value. No authorization is needed, however, to make a communication that falls within one of the exceptions to the marketing definition. An authorization for marketing that involves the covered entity's receipt of direct or indirect remuneration from a third party must reveal that fact. See OCR "Marketing" Guidance.
Limiting Uses and Disclosures to the Minimum Necessary	**Minimum Necessary.** A central aspect of the Privacy Rule is the principle of "minimum necessary" use and disclosure. A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request.[50] A covered entity must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. When the minimum necessary standard applies to a use or disclosure, a covered entity may not use, disclose, or request the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose. See OCR "Minimum Necessary" Guidance. The minimum necessary requirement is not imposed in any of the following circumstances: (a) disclosure to or a request by a health care provider for treatment; (b) disclosure to an individual who is the subject of the information, or the individual's personal representative; (c) use or disclosure made pursuant to an authorization; (d) disclosure to HHS for complaint investigation, compliance review or enforcement; (e) use or disclosure that is required by law; or (f) use or disclosure required for compliance with the HIPAA Transactions Rule or other HIPAA Administrative Simplification Rules. **Access and Uses.** For internal uses, a covered entity must develop and implement policies and procedures that restrict access and uses of protected health information based on the specific roles of the members of their workforce. These policies and procedures must identify the persons, or classes of persons, in the workforce who need access to protected health information to carry out their duties, the categories of

	protected health information to which access is needed, and any conditions under which they need the information to do their jobs. **Disclosures and Requests for Disclosures.** Covered entities must establish and implement policies and procedures (which may be standard protocols) for *routine, recurring disclosures, or requests for disclosures,* that limits the protected health information disclosed to that which is the minimum amount reasonably necessary to achieve the purpose of the disclosure. Individual review of each disclosure is not required. For non-routine, non-recurring disclosures, or requests for disclosures that it makes, covered entities must develop criteria designed to limit disclosures to the information reasonably necessary to accomplish the purpose of the disclosure and review each of these requests individually in accordance with the established criteria. **Reasonable Reliance.** If another covered entity makes a request for protected health information, a covered entity may rely, if reasonable under the circumstances, on the request as complying with this minimum necessary standard. Similarly, a covered entity may rely upon requests as being the minimum necessary protected health information from: (a) a public official, (b) a professional (such as an attorney or accountant) who is the covered entity's business associate, seeking the information to provide services to or for the covered entity; or (c) a researcher who provides the documentation or representation required by the Privacy Rule for research.
Notice and Other Individual Rights	**Privacy Practices Notice.** Each covered entity, with certain exceptions, must provide a notice of its privacy practices.[51] The Privacy Rule requires that the notice contain certain elements. The notice must describe the ways in which the covered entity may use and disclose protected health information. The notice must state the covered entity's duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice. The notice must describe individuals' rights, including the right to complain to HHS and to the covered entity if they believe their privacy rights have been violated. The notice must include a point of contact for further information and for making complaints to the covered entity. Covered entities must act in accordance with their notices. The Rule also contains specific distribution requirements for direct treatment providers, all other health care providers, and health plans. See OCR "Notice" Guidance. • **Notice Distribution.** A covered health care provider with a *direct treatment relationship* with individuals must deliver a privacy practices notice to patients starting April 14, 2003 as follows: o Not later than the first service encounter by personal delivery (for patient visits), by automatic and contemporaneous electronic response (for electronic service delivery), and by prompt mailing (for telephonic service delivery); o By posting the notice at each service delivery site in a clear and prominent place where people seeking service may reasonably be expected to be able to read the notice; and o In emergency treatment situations, the provider must furnish its notice as soon as practicable after the emergency abates.

Covered entities, whether *direct treatment providers* or *indirect treatment providers* (such as laboratories) or *health plans* must supply notice to anyone on request.[52] A covered entity must also make its notice electronically available on any web site it maintains for customer service or benefits information.

The covered entities in an *organized health care arrangement* may use a joint privacy practices notice, as long as each agrees to abide by the notice content with respect to the protected health information created or received in connection with participation in the arrangement.[53] Distribution of a joint notice by any covered entity participating in the organized health care arrangement at the first point that an OHCA member has an obligation to provide notice satisfies the distribution obligation of the other participants in the organized health care arrangement.

A health plan must distribute its privacy practices notice to each of its enrollees by its Privacy Rule compliance date. Thereafter, the health plan must give its notice to each new enrollee at enrollment, and send a reminder to every enrollee at least once every three years that the notice is available upon request. A health plan satisfies its distribution obligation by furnishing the notice to the "named insured," that is, the subscriber for coverage that also applies to spouses and dependents.

- **Acknowledgement of Notice Receipt.** A covered health care provider with a direct treatment relationship with individuals must make a good faith effort to obtain written acknowledgement from patients of receipt of the privacy practices notice.[54] The Privacy Rule does not prescribe any particular content for the acknowledgement. The provider must document the reason for any failure to obtain the patient's written acknowledgement. The provider is relieved of the need to request acknowledgement in an emergency treatment situation.

Access. Except in certain circumstances, individuals have the right to review and obtain a copy of their protected health information in a covered entity's *designated record set*.[55] The "designated record set" is that group of records maintained by or for a covered entity that is used, in whole or part, to make decisions about individuals, or that is a provider's medical and billing records about individuals or a health plan's enrollment, payment, claims adjudication, and case or medical management record systems.[56] The Rule excepts from the right of access the following protected health information: psychotherapy notes, information compiled for legal proceedings, laboratory results to which the Clinical Laboratory Improvement Act (CLIA) prohibits access, or information held by certain research laboratories. For information included within the right of access, covered entities may deny an individual access in certain specified situations, such as when a health care professional believes access could cause harm to the individual or another. In such situations, the individual must be given the right to have such denials reviewed by a licensed health care professional for a second opinion.[57] Covered entities may impose reasonable, cost-based fees for the cost of copying and postage.

Amendment. The Rule gives individuals the right to have covered entities amend their protected health information in a designated record set when that information is

	inaccurate or incomplete.[58] If a covered entity accepts an amendment request, it must make reasonable efforts to provide the amendment to persons that the individual has identified as needing it, and to persons that the covered entity knows might rely on the information to the individual's detriment.[59] If the request is denied, covered entities must provide the individual with a written denial and allow the individual to submit a statement of disagreement for inclusion in the record. The Rule specifies processes for requesting and responding to a request for amendment. A covered entity must amend protected health information in its designated record set upon receipt of notice to amend from another covered entity. **Disclosure Accounting.** Individuals have a right to an accounting of the disclosures of their protected health information by a covered entity or the covered entity's business associates.[60] The maximum disclosure accounting period is the six years immediately preceding the accounting request, except a covered entity is not obligated to account for any disclosure made before its Privacy Rule compliance date. The Privacy Rule does not require accounting for disclosures: (a) for treatment, payment, or health care operations; (b) to the individual or the individual's personal representative; (c) for notification of or to persons involved in an individual's health care or payment for health care, for disaster relief, or for facility directories; (d) pursuant to an authorization; (e) of a limited data set; (f) for national security or intelligence purposes; (g) to correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody; or (h) incident to otherwise permitted or required uses or disclosures. Accounting for disclosures to health oversight agencies and law enforcement officials must be temporarily suspended on their written representation that an accounting would likely impede their activities. **Restriction Request.** Individuals have the right to request that a covered entity restrict use or disclosure of protected health information for treatment, payment or health care operations, disclosure to persons involved in the individual's health care or payment for health care, or disclosure to notify family members or others about the individual's general condition, location, or death.[61] A covered entity is under no obligation to agree to requests for restrictions. A covered entity that does agree must comply with the agreed restrictions, except for purposes of treating the individual in a medical emergency.[62] **Confidential Communications Requirements.** Health plans and covered health care providers must permit individuals to request an alternative means or location for receiving communications of protected health information by means other than those that the covered entity typically employs.[63] For example, an individual may request that the provider communicate with the individual through a designated address or phone number. Similarly, an individual may request that the provider send communications in a closed envelope rather than a post card. Health plans must accommodate reasonable requests if the individual indicates that the disclosure of all or part of the protected health information could endanger the individual. The health plan may not question the individual's statement of endangerment. Any covered entity may condition compliance with a confidential communication request on the individual specifying an alternative address or method of contact and explaining how any payment will be handled.

Administrative Requirements	HHS recognizes that covered entities range from the smallest provider to the largest, multi-state health plan. Therefore the flexibility and scalability of the Rule are intended to allow covered entities to analyze their own needs and implement solutions appropriate for their own environment. What is appropriate for a particular covered entity will depend on the nature of the covered entity's business, as well as the covered entity's size and resources. **Privacy Policies and Procedures.** A covered entity must develop and implement written privacy policies and procedures that are consistent with the Privacy Rule.[64] **Privacy Personnel.** A covered entity must designate a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the covered entity's privacy practices.[65] **Workforce Training and Management.** Workforce members include employees, volunteers, trainees, and may also include other persons whose conduct is under the direct control of the entity (whether or not they are paid by the entity).[66] A covered entity must train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions.[67] A covered entity must have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures or the Privacy Rule.[68] **Mitigation.** A covered entity must mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule.[69] **Data Safeguards.** A covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure.[70] For example, such safeguards might include shredding documents containing protected health information before discarding them, securing medical records with lock and key or pass code, and limiting access to keys or pass codes. See OCR "Incidental Uses and Disclosures" Guidance. **Complaints.** A covered entity must have procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule.[71] The covered entity must explain those procedures in its privacy practices notice.[72] Among other things, the covered entity must identify to whom individuals can submit complaints to at the covered entity and advise that complaints also can be submitted to the Secretary of HHS. **Retaliation and Waiver.** A covered entity may not retaliate against a person for exercising rights provided by the Privacy Rule, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Rule.[73] A covered entity may not

	require an individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.[74] **Documentation and Record Retention.** A covered entity must maintain, until six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented.[75] **Fully-Insured Group Health Plan Exception.** The only administrative obligations with which a fully-insured group health plan that has no more than enrollment data and summary health information is required to comply are the (1) ban on retaliatory acts and waiver of individual rights, and (2) documentation requirements with respect to plan documents if such documents are amended to provide for the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO that services the group health plan.[76]
Organizational Options	The Rule contains provisions that address a variety of organizational issues that may affect the operation of the privacy protections. **Hybrid Entity.** The Privacy Rule permits a covered entity that is a single legal entity and that conducts both covered and non-covered functions to elect to be a "hybrid entity."[77] (The activities that make a person or organization a covered entity are its "covered functions."[78]) To be a hybrid entity, the covered entity must designate in writing its operations that perform covered functions as one or more "health care components." After making this designation, most of the requirements of the Privacy Rule will apply only to the health care components. A covered entity that does not make this designation is subject in its entirety to the Privacy Rule. **Affiliated Covered Entity.** Legally separate covered entities that are affiliated by common ownership or control may designate themselves (including their health care components) as a single covered entity for Privacy Rule compliance.[79] The designation must be in writing. An affiliated covered entity that performs multiple covered functions must operate its different covered functions in compliance with the Privacy Rule provisions applicable to those covered functions. **Organized Health Care Arrangement.** The Privacy Rule identifies relationships in which participating covered entities share protected health information to manage and benefit their common enterprise as "organized health care arrangements."[80] Covered entities in an organized health care arrangement can share protected health information with each other for the arrangement's joint health care operations.[81] **Covered Entities With Multiple Covered Functions.** A covered entity that performs multiple covered functions must operate its different covered functions in compliance with the Privacy Rule provisions applicable to those covered functions.[82] The covered entity may not use or disclose the protected health information of an individual who receives services from one covered function (e.g., health care provider) for another covered function (e.g., health plan) if the individual is not involved with the other function.

	Group Health Plan disclosures to Plan Sponsors. A group health plan and the health insurer or HMO offered by the plan may disclose the following protected health information to the "plan sponsor"—the employer, union, or other employee organization that sponsors and maintains the group health plan[83]: • Enrollment or disenrollment information with respect to the group health plan or a health insurer or HMO offered by the plan. • If requested by the plan sponsor, summary health information for the plan sponsor to use to obtain premium bids for providing health insurance coverage through the group health plan, or to modify, amend, or terminate the group health plan. "Summary health information" is information that summarizes claims history, claims expenses, or types of claims experience of the individuals for whom the plan sponsor has provided health benefits through the group health plan, and that is stripped of all individual identifiers other than five digit zip code (though it need not qualify as de-identified protected health information). • Protected health information of the group health plan's enrollees for the plan sponsor to perform plan administration functions. The plan must receive certification from the plan sponsor that the group health plan document has been amended to impose restrictions on the plan sponsor's use and disclosure of the protected health information. These restrictions must include the representation that the plan sponsor will not use or disclose the protected health information for any employment-related action or decision or in connection with any other benefit plan.
Other Provisions: Personal Representatives and Minors	**Personal Representatives.** The Privacy Rule requires a covered entity to treat a *"personal representative"* the same as the individual, with respect to uses and disclosures of the individual's protected health information, as well as the individual's rights under the Rule.[84] A personal representative is a person legally authorized to make health care decisions on an individual's behalf or to act for a deceased individual or the estate. The Privacy Rule permits an exception when a covered entity has a reasonable belief that the personal representative may be abusing or neglecting the individual, or that treating the person as the personal representative could otherwise endanger the individual. **Special case: Minors.** In most cases, parents are the personal representatives for their minor children. Therefore, in most cases, parents can exercise individual rights, such as access to the medical record, on behalf of their minor children. In certain exceptional cases, the parent is not considered the personal representative. In these situations, the Privacy Rule defers to State and other law to determine the rights of parents to access and control the protected health information of their minor children. If State and other law is silent concerning parental access to the minor's protected health information, a covered entity has discretion to provide or deny a parent access to the minor's health information, provided the decision is made by a licensed health care professional in the exercise of professional judgment. See OCR "Personal Representatives" Guidance.

State Law	**Preemption.** In general, State laws that are contrary to the Privacy Rule are preempted by the federal requirements, which means that the federal requirements will apply.[85] "Contrary" means that it would be impossible for a covered entity to comply with both the State and federal requirements, or that the provision of State law is an obstacle to accomplishing the full purposes and objectives of the Administrative Simplification provisions of HIPAA.[86] The Privacy Rule provides exceptions to the general rule of federal preemption for contrary State laws that (1) relate to the privacy of individually identifiable health information and provide greater privacy protections or privacy rights with respect to such information, (2) provide for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention, or (3) require certain health plan reporting, such as for management or financial audits. **Exception Determination.** In addition, preemption of a contrary State law will not occur if HHS determines, in response to a request from a State or other entity or person, that the State law: • Is necessary to prevent fraud and abuse related to the provision of or payment for health care, • Is necessary to ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation, • Is necessary for State reporting on health care delivery or costs, • Is necessary for purposes of serving a compelling public health, safety, or welfare need, and, if a Privacy Rule provision is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or • Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.
Enforcement and Penalties for Noncompliance	**Compliance.** Consistent with the principles for achieving compliance provided in the Rule, HHS will seek the cooperation of covered entities and may provide technical assistance to help them comply voluntarily with the Rule.[87] The Rule provides processes for persons to file complaints with HHS, describes the responsibilities of covered entities to provide records and compliance reports and to cooperate with, and permit access to information for, investigations and compliance reviews. **Civil Money Penalties.** HHS may impose civil money penalties on a covered entity of $100 per failure to comply with a Privacy Rule requirement.[88] That penalty may not exceed $25,000 per year for multiple violations of the identical Privacy Rule requirement in a calendar year. HHS may not impose a civil money penalty under specific circumstances, such as when a violation is due to reasonable cause and did not involve willful neglect and the covered entity corrected the violation within 30 days of when it knew or should have known of the violation.

	Criminal Penalties. A person who knowingly obtains or discloses individually identifiable health information in violation of HIPAA faces a fine of $50,000 and up to one-year imprisonment.[89] The criminal penalties increase to $100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to $250,000 and up to ten years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm. Criminal sanctions will be enforced by the Department of Justice.
Compliance Dates	**Compliance Schedule.** All covered entities, except "small health plans," must be compliant with the Privacy Rule by April 14, 2003.[90] Small health plans, however, have until April 14, 2004 to comply. **Small Health Plans.** A health plan with annual receipts of not more than $5 million is a small health plan.[91] Health plans that file certain federal tax returns and report receipts on those returns should use the guidance provided by the Small Business Administration at 13 Code of Federal Regulations (CFR) 121.104 to calculate annual receipts. Health plans that do not report receipts to the Internal Revenue Service (IRS), for example, group health plans regulated by the Employee Retirement Income Security Act 1974 (ERISA) that are exempt from filing income tax returns, should use proxy measures to determine their annual receipts.[92] See What constitutes a small health plan?
Copies of the Rule & Related Materials	The entire Privacy Rule, as well as guidance and additional materials, may be found on our website, http://www.hhs.gov/ocr/hipaa.

End Notes

[1] Pub. L. 104-191.

[2] 65 FR 82462.

[3] 67 FR 53182.

[4] 45 C.F.R. §§ 160.102, 160.103.

[5] Even if an entity, such as a community health center, does not meet the definition of a health plan, it may, nonetheless, meet the definition of a health care provider, and, if it transmits health information in electronic form in connection with the transactions for which the Secretary of HHS has adopted standards under HIPAA, may still be a covered entity.

[6] 45 C.F.R. §§ 160.102, 160.103; *see* Social Security Act § 1172(a)(3), 42 U.S.C. § 1320d-1(a)(3). The transaction standards are established by the HIPAA Transactions Rule at 45 C.F.R. Part 162.

[7] 45 C.F.R. § 160.103.

[8] 45 C.F.R. § 164.500(b).

[9] 45 C.F.R. § 160.103.

[10] 45 C.F.R. §§ 164.502(e), 164.504(e).

[11] 45 C.F.R. § 164.532

[12] 45 C.F.R. § 160.103.

[13] 45 C.F.R. § 160.103

[14] 45 C.F.R. §§ 164.502(d)(2), 164.514(a) and (b).

[15] The following identifiers of the individual or of relatives, employers, or household members of the individual must be removed to achieve the "safe harbor" method of de-identification: (A) Names; (B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of Census (1) the geographic units formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000; (C) All elements of dates (except year) for dates directly related to the individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older; (D) Telephone numbers; (E) Fax numbers; (F) Electronic mail addresses: (G) Social security numbers; (H) Medical record numbers; (I) Health plan beneficiary numbers; (J) Account numbers; (K) Certificate/license numbers; (L) Vehicle identifiers and serial numbers, including license plate numbers; (M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; (P) Biometric identifiers, including finger and voice prints; (Q) Full face photographic images and any comparable images; and ® any other unique identifying number, characteristic, or code, except as permitted for re-identification purposes provided certain conditions are met. In addition to the removal of the above-stated identifiers, the covered entity may not have actual knowledge that the remaining information could be used alone or in combination with any other information to identify an individual who is subject of the information. 45 C.F.R. § 164.514(b).

[16] 45 C.F.R. § 164.502(a).

[17] 45 C.F.R. § 164.502(a)(2).

[18] 45 C.F.R. § 164.502(a)(1).

[19] 45 C.F.R. § 164.506(c).

[20] 45 C.F.R. § 164.501.

[21] 45 C.F.R. § 164.501.

[22] 45 C.F.R. § 164.501.

[23] 45 C.F.R. § 164.508(a)(2)

[24] 45 C.F.R. § 164.506(b).

[25] 45 C.F.R. § 164.510(a).

[26] 45 C.F.R. § 164.510(b).

[27] 45 C.F.R. §§ 164.502(a)(1)(iii).

[28] *See* 45 C.F.R. § 164.512.

[29] 45 C.F.R. § 164.512(a).

[30] 45 C.F.R. § 164.512(b).

[31] 45 C.F.R. § 164.512(a), (c).

[32] 45 C.F.R. § 164.512(d).

[33] 45 C.F.R. § 164.512(e).

[34] 45 C.F.R. § 164.512(f).

[35] 45 C.F.R. § 164.512(g).

[36] 45 C.F.R. § 164.512(h).

[37] The Privacy Rule defines research as, "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." 45 C.F.R. § 164.501.

[38] 45 C.F.R. § 164.512(i).

[39] 45 CFR § 164.514(e).

[40] 45 C.F.R. § 164.512(j).

[41] 45 C.F.R. § 164.512(k).

[42] 45 C.F.R. § 164.512(l).

[43] 45 C.F.R. § 164.514(e). A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (i) Names; (ii) Postal address information, other than town or city, State and zip code; (iii) Telephone numbers; (iv) Fax numbers; (v) Electronic mail addresses: (vi) Social security numbers; (vii) Medical record numbers; (viii) Health plan beneficiary numbers; (ix) Account numbers; (x) Certificate/license numbers; (xi) Vehicle identifiers and serial numbers, including license plate numbers; (xii) Device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) Biometric identifiers, including finger and voice prints; (xvi) Full face photographic images and any comparable images. 45 C.F.R. § 164.514(e)(2).

[44] 45 C.F.R. § 164.508.

[45] A covered entity may condition the provision of health care solely to generate protected health information for disclosure to a third party on the individual giving authorization to disclose the

information to the third party. For example, a covered entity physician may condition the provision of a physical examination to be paid for by a life insurance issuer on an individual's authorization to disclose the results of that examination to the life insurance issuer. A health plan may condition enrollment or benefits eligibility on the individual giving authorization, requested before the individual's enrollment, to obtain protected health information (other than psychotherapy notes) to determine the individual's eligibility or enrollment or for underwriting or risk rating. A covered health care provider may condition treatment related to research (e.g., clinical trials) on the individual giving authorization to use or disclose the individual's protected health information for the research. 45 C.F.R. 508(b)(4).

[46] 45 CFR § 164.532.

[47] "Psychotherapy notes" means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date. 45 C.F.R. § 164.501.

[48] 45 C.F.R. § 164.508(a)(2).

[49] 45 C.F.R. §§ 164.501 and 164.508(a)(3).

[50] 45 C.F.R. §§ 164.502(b) and 164.514 (d).

[51] 45 C.F.R. §§ 164.520(a) and (b). A group health plan, or a health insurer or HMO with respect to the group health plan, that intends to disclose protected health information (including enrollment data or summary health information) to the plan sponsor, must state that fact in the notice. Special statements are also required in the notice if a covered entity intends to contact individuals about health-related benefits or services, treatment alternatives, or appointment reminders, or for the covered entity's own fundraising.

[52] 45 C.F.R. § 164.520(c).

[53] 45 C.F.R. § 164.520(d).

[54] 45 C.F.R. § 164.520(c).

[55] 45 C.F.R. § 164.524.

[56] 45 C.F.R. § 164.501.

[57] A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed by a licensed health care professional (who is designated by the covered entity and who did not participate in the original decision to deny), when a licensed health care professional has determined, in the exercise of professional judgment, that: (a) the access requested is reasonably likely to endanger the life or physical safety of the individual or another person; (b) the protected health information makes reference to another person (unless such other person is a health care provider) and the access requested is reasonably likely to cause substantial harm to such other person; or (c) the request for access is made by the individual's personal representative and the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

A covered entity may deny access to individuals, without providing the individual an opportunity for review, in the following protected situations: (a) the protected health information falls under an exception to the right of access; (b) an inmate request for protected health information under certain circumstances; (c) information that a provider creates or obtains in the course of research that includes treatment for which the individual has agreed not to have access as part of consenting

to participate in the research (as long as access to the information is restored upon completion of the research); (d) for records subject to the Privacy Act, information to which access may be denied under the Privacy Act, 5 U.S.C. § 552a; and (e) information obtained under a promise of confidentiality from a source other than a health care provider, if granting access would likely reveal the source. 45 C.F.R. § 164.524.

[58] 45 C.F.R. § 164.526.

[59] Covered entities may deny an individual's request for amendment only under specified circumstances. A covered entity may deny the request if it: (a) may exclude the information from access by the individual; (b) did not create the information (unless the individual provides a reasonable basis to believe the originator is no longer available); (c) determines that the information is accurate and complete; or (d) does not hold the information in its designated record set. 164.526(a)(2).

[60] 45 C.F.R. § 164.528.

[61] 45 C.F.R. § 164.522(a).

[62] 45 C.F.R. § 164.522(a). In addition, a restriction agreed to by a covered entity is not effective under this subpart to prevent uses or disclosures permitted or required under §§ 164.502(a)(2)(ii), 164.510(a) or 164.512.

[63] 45 C.F.R. § 164.522(b).

[64] 45 C.F.R. § 164.530(i).

[65] 45 C.F.R. § 164.530(a).

[66] 45 C.F.R. §160.103.

[67] 45 C.F.R. § 164.530(b).

[68] 45 C.F.R. § 164.530(e).

[69] 45 C.F.R. § 164.530(f).

[70] 45 C.F.R. § 164.530(c).

[71] 45 C.F.R. § 164.530(d).

[72] 45 C.F.R. § 164.520(b)(1)(vi).

[73] 45 C.F.R. § 164.530(g).

[74] 45 C.F.R. § 164.530(h).

[75] 45 C.F.R. § 164.530(j).

[76] 45 C.F.R. § 164.530(k).

[77] 45 C.F.R. §§ 164.103, 164.105.

[78] 45 C.F.R. § 164.103.

[79] 45 C.F.R. §164.105. Common ownership exists if an entity possesses an ownership or equity interest of five percent or more in another entity; common control exists if an entity has the direct or indirect power significantly to influence or direct the actions or policies of another entity. 45 C.F.R. §§ 164.103.

[80] The Privacy Rule at 45 C.F.R. § 160.103 identifies five types of organized health care arrangements:

- A clinically-integrated setting where individuals typically receive health care from more than one provider.
- An organized system of health care in which the participating covered entities hold themselves out to the public as part of a joint arrangement and jointly engage in

utilization review, quality assessment and improvement activities, or risk-sharing payment activities.

- A group health plan and the health insurer or HMO that insures the plan's benefits, with respect to protected health information created or received by the insurer or HMO that relates to individuals who are or have been participants or beneficiaries of the group health plan.
- All group health plans maintained by the same plan sponsor.
- All group health plans maintained by the same plan sponsor and all health insurers and HMOs that insure the plans' benefits, with respect to protected health information created or received by the insurers or HMOs that relates to individuals who are or have been participants or beneficiaries in the group health plans.

[81] 45 C.F.R. § 164.506(c)(5).

[82] 45 C.F.R. § 164.504(g).

[83] 45 C.F.R. § 164.504(f).

[84] 45 C.F.R. § 164.502(g).

[85] 45 C.F.R. §160.203.

[86] 45 C.F.R. § 160.202.

[87] 45 C.F.R.§ 160.304

[88] Pub. L. 104-191; 42 U.S.C. §1320d-5.

[89] Pub. L. 104-191; 42 U.S.C. §1320d-6.

[90] 45 C.F.R. § 164.534.

[91] 45 C.F.R. § 160.103.

[92] Fully insured health plans should use the amount of total premiums that they paid for health insurance benefits during the plan's last full fiscal year. Self-insured plans, both funded and unfunded, should use the total amount paid for health care claims by the employer, plan sponsor or benefit fund, as applicable to their circumstances, on behalf of the plan during the plan's last full fiscal year. Those plans that provide health benefits through a mix of purchased insurance and self-insurance should combine proxy measures to determine their total annual receipts.

Attachment D

MEDICAID, TITLE XIX OF THE SOCIAL SECURITY ACT

TABLE OF CONTENTS OF TITLE[2]

MEDICAID AND CHIP PAYMENT AND ACCESS COMMISSION[3]

Sec. 1900. **[**42 U.S.C. 1396–1**]** (a) Establishment.—There is hereby established the Medicaid and CHIP Payment and Access Commission (in this section referred to as "MACPAC").

(b) Duties.—

(1) Review of access policies for all states and annual reports.—MACPAC shall—

(A) review policies of the Medicaid program established under this title (in this section referred to as "Medicaid") and the State Children's Health Insurance Program established under title XXI (in this section referred to as "CHIP") affecting access to covered items and services, including topics described in paragraph (2);

(B) make recommendations to Congress, the Secretary, and the Statesconcerning such access policies;

(C) by not later than March 15 of each year (beginning with 2010), submit a report to Congress containing the results of such reviews and MACPAC's recommendations concerning such policies; and

(D) by not later than June 15 of each year (beginning with 2010), submit a report to Congress containing an examination of issues affecting Medicaid and CHIP, including the implications of changes in health care delivery in the United States and in the market for health care services on such programs.

(2) Specific topics to be reviewed.—Specifically, MACPAC shall review and assess the following:

(A) Medicaid and chip payment policies.—Payment policies under Medicaid and CHIP, including—

(i) the factors affecting expenditures for the efficient provision ofitems and services in different sectors, including the process for updating payments to medical, dental, and health professionals, hospitals, residential and long-term care providers, providers of home and community based services, Federally-qualified health centers and rural health clinics, managed care entities, and providers of other covered items and services;

(ii) payment methodologies; and

(iii) the relationship of such factors and methodologies to access and quality of care for Medicaid and CHIP beneficiaries (including how such factors and methodologies enable such beneficiaries to obtain the services for which they are eligible, affect provider supply, and affect providers that serve a disproportionate share of low-income and other vulnerable populations).

(B) Eligibility policies.—Medicaid and CHIP eligibility policies, including a determination of the degree to which Federal and State policies provide health care coverage to needy populations.

(C) Enrollment and retention processes.— Medicaid and CHIP enrollment and retention processes, including a determination of the degree to which Federal and State policies encourage the enrollment of individuals who are eligible for such programs and screen out individuals who are ineligible, while minimizing the share of program expenses devoted to such processes.

(D) coverage policiesMedicaid and CHIP benefit and coverage policies, including a determination of the degree to which Federal and State policies provide access to the services enrollees require to improve and maintain their health and functional status.

(E) Quality of care.—Medicaid and CHIP policies as they relate to the quality of care provided under those programs, including a determination of the degree to which Federal and State policies achieve their stated goals and

(F) Interaction of medicaid and chip payment policies with health care delivery generally.—The effect of Medicaid and CHIP payment policies on access to items and services for children and other Medicaid and CHIP populations other than under this title or title XXI and the implications of changes in health care delivery in the United States and in the general market for health care items and services on Medicaid and CHIP.

(G) Interactions with medicare and medicaid.—)consistent with paragraph (11), the interaction of policies under Medicaid and the Medicare program under title XVIII, including with respect to how such interactions affect access to services, payments, and dual eligible individuals.

(H) Other access policies.—The effect of other Medicaid and CHIP policies on access to covered items and services, including policies relating to transportation and language barriers and preventive, acute, and long-term services and supports.

(3) Recommendations and reports.—

(A) review national and State-specific Medicaid and CHIP data; and

(B) submit reports and recommendations to Congress, the Secretary, and States based on such reviews.

(4) Creation of early-warning system.—MACPAC shall create an early-warning system to identify provider shortage areas , as well as other factors that adversely affect, or have the potential to adversely affect, access to care by, or the health care status of, Medicaid and CHIP beneficiaries. MACPAC shall include in the annual report required under paragraph (1)(D) a description of all such areas or problems identified with respect to the period addressed in the report.

(5)

(A) Comments on certain secretarial reports and regulations.—.If the Secretary submits to Congress (or a committee of Congress) a report that is required by law and that relates to access policies, including with respect to payment policies, under Medicaid or CHIP, the Secretary shall transmit a copy of the report to MACPAC. MACPAC shall review the report and, not later than 6 months after the date of submittal of

the Secretary's report to Congress, shall submit to the appropriate committees of Congress and the Secretary written comments on such report. Such comments may include such recommendations as MACPAC deems appropriate.

(B) Regulations.—MACPAC shall review Medicaid and CHIP regulations and may comment through submission of a report to the appropriate committees of Congress and the Secretary, on any such regulations that affect access, quality, or efficiency of health care.

(6) Agenda and additional reviews.—

(A) In general.— MACPAC shall consult periodically with the chairmen and ranking minority members of the appropriate committees of Congress regarding MACPAC's agenda and progress towards achieving the agenda. MACPAC may conduct additional reviews, and submit additional reports to the appropriate committees of Congress, from time to time on such topics relating to the program under this title or title XXI as may be requested by such chairmen and members and as MACPAC deems appropriate.

(B) Review and reports regarding medicaid dsh.—

(i) In general.— MACPAC shall review and submit an annual report to Congress on disproportionate share hospital payments under section 1923. Each report shall include the information specified in clause (ii).

(ii) Required report information.—Each report required under this subparagraph shall include the following:

(I) Data relating to changes in the number of uninsured individuals.

(II) Data relating to the amount and sources of hospitals' uncompensated care costs, including the amount of such costs that are the result of providing unreimbursed or under-reimbursed services, charity care, or bad debt.

(III) Data identifying hospitals with high levels of uncompensated care that also provide access to essential community services for low-income, uninsured, and vulnerable populations, such as graduate medical education, and the continuum of primary through quarternary care, including the provision of trauma care and public health services.

(IV) State-specific analyses regarding the relationship between the most recent State DSH allotment and the projected State DSH allotment for the succeeding year and the data reported under subclauses (I), (II), and (III) for the State.

(iii) Data.—Notwithstanding any other provision of law, the Secretary regularly shall provide MACPAC with the most recent State reports and most recent independent certified audits submitted under section 1923(j), cost reports submitted under title XVIII, and such other data as MACPAC may request for purposes of conducting the reviews and preparing and submitting the annual reports required under this subparagraph.

(iv) Submission deadlines.— The first report required under this subparagraph shall be submitted to Congress not later than February 1, 2016. Subsequent reports shall be submitted as part of, or with, each annual report required under paragraph (1)(C) during the period of fiscal years 2017 through 2024.[4]

(7) Availability of reports.—MACPAC shall transmit to the Secretary a copy of each report submitted under this subsection and shall make such reports available to the public.

(8) Appropriate committee of congress.—For purposes of this section, the term "appropriate committees of Congress" means the Committee on Energy and Commerce of the House of Representatives and the Committee on Finance of the Senate.

(9) Voting and reporting requirements.—With respect to each recommendation contained in a report submitted under paragraph (1), each member of MACPAC shall vote on the recommendation, and MACPAC shall include, by member, the results of that vote in the report containing the recommendation.

(10) Examination of budget consequences.—Before making any recommendations, MACPAC shall examine the budget consequences of such recommendations, directly or through consultation with appropriate expert entities, and shall submit with any recommendations, a report on the Federal and State-specific budget consequences of the recommendations.

(11) Consultation and coordination with medpac.—

(A) In general.—MACPAC shall consult with the Medicare Payment Advisory Commission (in this paragraph referred to as 'MedPAC') established under section 1805 in carrying out its duties under this section, as appropriate and particularly with respect to the issues specified in paragraph (2) as they relate to those Medicaid beneficiaries who are dually eligible for Medicaid and the Medicare program under title XVIII, adult Medicaid beneficiaries (who are not dually eligible for Medicare), and beneficiaries under Medicare. Responsibility for analysis of and recommendations to change Medicare policy regarding Medicare beneficiaries, including Medicare beneficiaries who are dually eligible for Medicare and Medicaid, shall rest with MedPAC.

(B) Information sharing.—MACPAC and MedPAC shall have access to deliberations and records of the other such entity, respectively, upon the request of the other such entity.

(12) Consultation.—MACPAC shall regularly consult with States in carrying out its duties under this section, including with respect to developing processes for carrying out such duties, and shall ensure that input from States is taken into account and represented in MACPAC's recommendations and reports.

(13) Coordinate and consult with the federal coordinated health care office.—MACPAC shall coordinate and consult with the Federal Coordinated Health Care Office established under section 2081 of the Patient Protection and Affordable Care Act before making any recommendations regarding dual eligible individuals.

(14) Programmatic oversight vested in the secretary.—MACPAC's authority to make recommendations in accordance with this section shall not affect, or be considered to duplicate, the Secretary's authority to carry out Federal responsibilities with respect to Medicaid and CHIP.

(c) Membership.—

(1) Number and appointment.—MACPAC shall be composed of 17 members appointed by the Comptroller General of the United States.

(2) Qualifications.—

(A) In general.— The membership of MACPAC shall include individuals who have had direct experience as enrollees or parents or caregivers of enrollees in Medicaid or CHIP and individuals with national recognition for their expertise in Federal safety net health programs, health finance and economics, actuarial science, health plans and integrated delivery systems, reimbursement for health care, health information technology, and other providers of health services, public health, and other related fields, who provide a mix of different professions, broad geographic representation, and a balance between urban and rural representation.

(B) Inclusion.—The membership of MACPAC shall include (but not be limited to) physicians, dentists, and other health professionals, employers, third-party payers, and individuals with expertise in the delivery of health services. Such membership shall also include representatives of children, pregnant women, the elderly, individuals with disabilities, caregivers, and dual eligible individuals, current or former representatives of State agencies responsible for administering Medicaid, and current or former representatives of State agencies responsible for administering CHIP.

(C) Majority nonproviders.—Individuals who are directly involved in the provision, or management of the delivery, of items and services covered under Medicaid or CHIP shall not constitute a majority of the membership of MACPAC.

(D) Ethical disclosure.—The Comptroller General of the United States shall establish a system for public disclosure by members of MACPAC of financial and other potential conflicts of interest relating to such members. Members of MACPAC shall be treated as employees of Congress for purposes of applying title I of the Ethics in Government Act of 1978 (Public Law 95-521).

(3) Terms.—

(A) In general.—The terms of members of MACPAC shall be for 3 years except that the Comptroller General of the United States shall designate staggered terms for the members first appointed.

(B) Vacancies.—Any member appointed to fill a vacancy occurring before the expiration of the term for which the member's predecessor was appointed shall be appointed only for the remainder of that term. A member may serve after the expiration of that member's term until a successor has taken office. A vacancy in MACPAC shall be filled in the manner in which the original appointment was made.

(4) Compensation.—While serving on the business of MACPAC (including travel time), a member of MACPAC shall be entitled to compensation at the per diem equivalent of the rate provided for level IV of the Executive Schedule under section 5315 of title 5, United States Code; and while so serving away from home and the member's regular place of business, a member may be allowed travel expenses, as authorized by the Chairman of MACPAC. Physicians serving as personnel of MACPAC may be provided a physician comparability allowance by MACPAC in the same manner as Government physicians may be provided such an allowance by an agency under section 5948 of title 5, United States Code, and for such purpose subsection (i) of such section shall apply to MACPAC in the same manner as it applies to the

Tennessee Valley Authority. For purposes of pay (other than pay of members of MACPAC) and employment benefits, rights, and privileges, all personnel of MACPAC shall be treated as if they were employees of the United States Senate.

(5) Chairman; vice chairman.—The Comptroller General of the United States shall designate a member of MACPAC, at the time of appointment of the member as Chairman and a member as Vice Chairman for that term of appointment, except that in the case of vacancy of the Chairmanship or Vice Chairmanship, the Comptroller General of the United States may designate another member for the remainder of that member's term.

(6) Meetings.—MACPAC shall meet at the call of the Chairman.

(d) Director and Staff; Experts and Consultants.—Subject to such review as the Comptroller General of the United States deems necessary to assure the efficient administration of MACPAC, MACPAC may—

(1) employ and fix the compensation of an Executive Director (subject to the approval of the Comptroller General of the United States) and such other personnel as may be necessary to carry out its duties (without regard to the provisions of title 5, United States Code, governing appointments in the competitive service);

(2) seek such assistance and support as may be required in the performance of its duties from appropriate Federal and State departments and agencies;

(3) enter into contracts or make other arrangements, as may be necessary for the conduct of the work of MACPAC (without regard to section 3709 of the Revised Statutes (41 U.S.C. 5));

(4) make advance, progress, and other payments which relate to the work of MACPAC;

(5) provide transportation and subsistence for persons serving without compensation; and

(6) prescribe such rules and regulations as it deems necessary with respect to the internal organization and operation of MACPAC.

(e) Powers.—

(1) Obtaining official data.—MACPAC may secure directly from any department or agency of the United States and, as a condition for receiving payments under sections 1903(a) and 2105(a), from any State agency responsible for administering Medicaid or CHIP,information necessary to enable it to carry out this section. Upon request of the Chairman, the head of that department or agency shall furnish that information to MACPAC on an agreed upon schedule.

(2) Data collection.—In order to carry out its functions, MACPAC shall—

(A) utilize existing information, both published and unpublished, where possible, collected and assessed either by its own staff or under other arrangements made in accordance with this section;

(B) carry out, or award grants or contracts for, original research and experimentation, where existing information is inadequate; and

(C) adopt procedures allowing any interested party to submit information for MACPAC's use in making reports and recommendations.

(3) Access of gao to information.— The Comptroller General of the United States shall have unrestricted access to all deliberations, records, and nonproprietary data of MACPAC, immediately upon request.

(4) Periodic audit.—MACPAC shall be subject to periodic audit by the Comptroller General of the United States.

(f) Funding.—

(1) Request for appropriations.—MACPAC shall submit requests for appropriations (other than for fiscal year 2010) in the same manner as the Comptroller General of the United States submits requests for appropriations, but amounts appropriated for MACPAC shall be separate from amounts appropriated for the Comptroller General of the United States.

(2) Authorization.—There are authorized to be appropriated such sums as may be necessary to carry out the provisions of this section.

(3) Funding for fiscal year 2010.—

(A) In general.—Out of any funds in the Treasury not otherwise appropriated, there is appropriated to MACPAC to carry out the provisions of this section for fiscal year 2010, $9,000,000.

(B) Transfer of funds.—Notwithstanding section 2104(a)(13), from the amounts appropriated in such section for fiscal year 2010, $2,000,000 is hereby transferred and made available in such fiscal year to MACPAC to carry out the provisions of this section.

(4) Availability.—Amounts made available under paragraphs (2) and (3) to MACPAC to carry out the provisions of this section shall remain available until expended.

---

[1] Title XIX of the Social Security Act is administered by the Centers for Medicare and Medicaid Services.

Title XIX appears in the United States Code as §§1396–1396v, subchapter XIX, chapter 7, Title 42.

Regulations relating to Title XIX are contained in chapter IV, Title 42, and subtitle A, Title 45, Code of Federal Regulations.

See Vol. II, 31 U.S.C. 6504–6505 with respect to intergovernmental cooperation. See Vol. II, 31 U.S.C. 7501-7507 with respect to uniform audit requirements for State and local governments receiving Federal financial assistance.

See Vol. II, P.L. 78-410, §317A(a) and (d), with respect to coordination required in lead poisoning prevention; §353(i)(3) and (n), with respect to clinical laboratories; and, §399HH, with respect to a national strategy for quality improvement in health care.and §1301(c)(3), with respect to the requirement that health maintenance organizations enroll individuals entitled to medical assistance under Title XIX.

See Vol. II, P.L. 79-396, §17(p), with respect to proprietary title XIX center.

See Vol. II, P.L. 88-352, §601, for prohibition against discrimination in federally assisted programs.

See Vol. II, P.L. 89-73, §§203 and §306(c) with respect to agreements with other agencies.

See Vol. II, P.L. 94-566, §503, with respect to preservation of medicaid eligibility for individuals who cease to be eligible for supplemental security income benefits on account of cost-of-living increases in social security benefits.

See Vol. II, P.L. 99-319, §105, with respect to requirements for a system established regarding the rights of individuals with mental illness.

See Vol. II, P.L. 100-203, §4211(j) with respect to technical assistance with respect to the development and implementation of reimbursement methods for nursing facilities.

See Vol. II, P.L. 100-204, §724(d), with respect to furnishing information to the United States Commission on Improving the Effectiveness of the United Nations; and §725(b), with respect to the detailing of Government personnel.

See Vol. II, P.L. 100-235, §§5-8, with respect to responsibilities of each Federal agency for computer systems security and privacy.

See Vol. II, P.L. 100-690, §2306(c)(4), with respect to services covered in the plan of Hawaii; and §5301(a)(1)(C) and (d)(1)(B), with respect to benefits of drug traffickers and possessors.

See Vol. II, P.L. 101-121, with respect to the amounts collected by the Secretary of Health and Human Services under the authority of title IV of the Indian Health Care Improvement Act.

See Vol. II, P.L. 101-239, §6507, with respect to research on infant mortality and medicaid services; §6509, with respect to a maternal and child health handbook.

See Vol. II, P.L. 101-508, §4401(d), with respect to an annual report on drug pricing; §13302, with respect to protection of OASDI Trust Funds in the House of Representatives.

See Vol. II, P.L. 104-191, §261, with respect to purpose of administrative simplification.

See Vol. II, P.L. 104-193, §115, with respect to denial of assistance and benefits for certain drug-related convictions; §§401, 402, and 403, with respect to eligibility of aliens for certain Federal programs; and §911, with respect to fraud under means-tested welfare and public assistance programs.

See Vol. II, P.L. 110-90, §4, with respect to the extension of the SSI Web-based Asset Demonstration Project to the Medicaid program.

See Vol. II, P.L. 110-173, §206, with respect to a moratorium on certain payment restrictions.

See Vol. II, P.L. 110-252, §7001(a)(3), with respect to additional moratoria regarding the Medicaid program and §7001(b), with respect to funds to reduce Medicaid fraud and abuse.

See Vol. II, P.L. 111-148, §1103, with respect to immediate information that allows consumers to identify affordable coverage options; §1418, with respect to streamlining of procedures for enrollment through an exchange and State Medicaid, CHIP, and health subsidy programs; and §2602, with respect to providing Federal coverage and payment coordination for dual eligible beneficiaries; and P.L. 112-240,.§643, with respect to a commission on long-term care.

[2] This table of contents does not appear in the law.

[3] See Vol. II, P.L. 111-3, §506(b), with respect to the deadline for initial appointments and §506(c), with respect to an annual report on Medicaid.

[4] P.L. 113-93, §221(b)(1–2), revised paragraph (b)(6) into 2 subparagraphs, adding subparagraph (B). Effective April 1, 2014.

Attachment E

MEDICARE TITLE XVIII SOCIAL SECURITY ACT, TABLE OF CONTENTS OF TITLE[2]

---

[1] Title XVIII of the Social Security Act is administered by the Centers for Medicare and Medicaid Services.

Title XVIII appears in the United States Code as §§1395-1395ccc, subchapter XVIII, chapter 7, Title 42.

Regulations of the Secretary of Health and Human Services relating to Title XVIII are contained in chapter IV, Title 42, and in subtitle A, Title 45, Code of Federal Regulations.

See Vol. II, 31 U.S.C. 3716(c)(3)(D), with respect to the application of administrative offset provisions to Medicare provider or supplier payments; P.L. 78-410, §353(i)(3) and (n), with respect to clinical laboratories; P.L. 88-352, §601, for prohibition against discrimination in Federally assisted programs; P.L. 89-73, §§203 and 422(c), with respect to consultation with respect to programs and services for the aged; P.L. 93-288, §312(d), with respect to exclusion from income and resources of certain Federal major disaster and emergency assistance; P.L. 97-248, §119, with respect to private sector review initiative and restriction against recovery from beneficiaries; P.L. 98-369, §2355, with respect to waivers for social health maintenance organizations; P.L. 99-177, §257(b)(3) and (c)(3), with respect to the calculation of the baseline; P.L. 99-272, §9220, with respect to extension, terms, conditions, and period of approval of the extension of On Lok waiver; and §9215, with respect to the extension of certain medicare health services demonstration projects; P.L. 99-319, §105, with respect to systems requirements; P.L. 99-509, §9339(d) with respect to State standards for directors of clinical laboratories; §9342 with respect to Alzheimer's disease demonstration projects; §9353(a)(4) with respect to a small-area analysis; and §9412 with respect to the waiver authority for chronically mentally ill and frail elderly; P.L. 99-660, Title IV, with respect to professional review activities; P.L. 100-203, §4008(d)(3), with respect to a report regarding hospital outlier payments; P.L. 100-204, §724(d), with respect to furnishing information to the United States Commission on Improving the Effectiveness of the United Nations; and §725(b), with respect to the detailing of Government personnel; P.L. 100-235, §§5–8, with respect to responsibilities of each Federal agency for computer systems security and privacy; P.L. 100-383, §§105(f)(2) and 206(d)(2), with respect to exclusions from income and resources of certain payments to certain individuals; P.L. 100-581, §§501, 502(b)(1), and 503, with respect to exclusion from income and resources of certain judgment funds; P.L. 100-647, §8411, with respect to treatment of certain nursing education programs; P.L. 100-690, §5301(a)(1)(C) and (d)(1)(B), with respect to benefits of drug traffickers and possessors; P.L. 100-713, §712, with respect to the provision of services in Montana; P.L. 101-121, with respect to the amounts collected by the Secretary of Health and Human Services under the authority of title IV of the Indian Health Care Improvement Act; P.L. 101-239, §6025, with respect to a dentist's serving as

hospital medical director; §6205(a)(1)(A) and (a)(2), with respect to recognition of costs of certain hospital-based nursing schools; P.L. 104-191, §261, with respect to purpose of administrative simplification; P.L. 106-554, §1(a)(6) [122], with respect to cancer prevention and treatment demonstrations for ethnic and racial minorities; and [128] with respect to a lifestyle modification program demonstration; P.L. 110-275, §186, with respect to a demonstration project to improve care to previously uninsured; P.L. 111-148, §1103, with respect to immediate information that allows consumers to identify affordable coverage options; §2602, with respect to providing Federal coverage and payment coordination for dual eligible beneficiaries; P.L. 111-240, §4241, with respect to the use of predictive modeling and other analytics technologies to identify and prevent waste, fraud, and abuse in the medicare fee-for-service program; P.L. 111-309, §206, with respect to funding for claims reprocessing; and P.L. 112-240, §609 (b), with respect to a strategy for providing data for performance improvement in a timely manner to applicable providers under the Medicare program and .§643, with respect to a commission on long-term care.

[2] This table of contents does not appear in the law.