COMPLIANCE PLAN

Adopted

December 9, 2015

Contents

1. Standards of Conduct and Compliance Policies Regarding Fraud and Abuse

A. Compliance Introduction and Mission

The mission of White River Health System, Inc.("WRHS") is to provide a safe, efficient delivery of quality healthcare and to improve the health of communities through education and outreach. To evidence this dedication, WRHS 's Board of Directors have adopted, developed, and implemented the Compliance Plan.

The Compliance Plan is intended to become a part of the fabric of the WRHS's routine operations and supplement the facility's Code of Conduct. WRHS communicates to all personnel its intent to comply with applicable state and federal laws through the Compliance Plan. In addition, the Compliance Plan will:

- Assess WRHS 's business activities and consequent legal risks.
- Educate all employees regarding compliance requirements and train employees to conduct their job activities in compliance with state and federal laws and regulations and according to the policies and procedures of the Compliance Plan.
- Implement monitoring and reporting functions, including auditing, to measure the effectiveness of the Plan and to address issues in an efficient and timely manner.
- Include enforcement and discipline components that encourage all employees to take their compliance responsibilities seriously.

Because of the extreme importance WRHS places on understanding and abiding by all applicable state and federal laws and regulations and acting in accordance with its standards and procedures, the Compliance Plan will be provided to all administrators, employees, members of the medical staff, and, upon request, to contractors, vendors, and suppliers (hereinafter collectively referred to as "WRHS Representatives").

No WRHS Representative has the authority to act contrary to any provision of the Compliance Plan or to condone any such violation by others. Any WRHS Representative with knowledge of information concerning a suspected violation of law or regulation or violation of a provision of the Compliance Plan is required to report promptly such violations via the Compliance Hotline described herein.

Employees who violate any provision of the Compliance Plan, including the duty to report suspected violations, shall be subject to disciplinary measures as set forth in the Plan. WRHS will take steps to investigate all reported violations pursuant to its Compliance Officer Protocol and Procedures and will endeavor to maintain an effective Compliance Plan that prevents, detects, and, eliminates violations of the law and regulations. In addition, promotion of and adherence to the Compliance Plan will be part of the job performance evaluation criteria for all employees.

WRHS will communicate changes to or modification of the Compliance Plan concurrent with or prior to the implementation of such changes or modifications; however, WRHS reserves the right to change, modify, or amend the Compliance Plan or any compliance polices as deemed necessary by WRHS without notice to Corporation Representatives or other persons.

Should WRHS Representatives have any questions or uncertainties regarding compliance with applicable state or federal law or regulations, or any aspect of the Compliance Plan, including a related policy or procedures, they should seek immediate clarification from the Compliance Officer (CO) or his/her designee.

B. Policy to Prevent Healthcare Fraud and Abuse

WRHS is committed to preventing health care fraud and abuse and complying with applicable State and Federal law related to health care fraud and abuse. This Policy is designed to detect and prevent fraud and abuse in our Health System and sets forth an overview of key provisions of the False Claims Act and other laws dealing with fraud and abuse and whistleblower protections for reporting those issues, as required by section 6032 of the Deficit Reduction Act of 2005.

All officers, directors, employees, contractors and agents of White River Health System will be provided with information about this Policy and will be expected to comply with its provisions in order to prevent and detect health care fraud and abuse.

Set forth below are summaries of Federal and State laws that provide liability for submission of false claims. These summaries are not intended to identify all applicable laws but rather to outline some of the major statutory provisions as required by the Deficit Reduction Act of 2005.

Federal False Claims Laws:

1. False Claims Act; 31 U.S.C. §§ 3729 -3733

The Federal False Claims Act ("FCA") applies to claims presented for payment by Federal health care programs and prohibits the knowing submission of unjustified or false claims to obtain Federal funds. Violations of the FCA include:

- Knowingly filing a false or fraudulent claim for payment to Medicare, Medicaid or other Federally funded health care program;
- Knowingly using a false record or statement to obtain payment on a false or fraudulent claim from Medicare, Medicaid or other Federally funded health care program; or
- Conspiring to defraud Medicare, Medicaid or other Federally funded health care program by attempting to have a false or fraudulent claim paid.

"Knowingly" Means:

- Actual knowledge that the information on the claim is false;
- Acting in deliberate ignorance of whether the claims is true or false; or
- Acting in reckless disregard of whether the claim is true or false.

Proof of specific intent to defraud is not required.

Punishment includes civil money penalties from $5,500 to $11,000 per violation, plus three times the amount of damages that the government sustained because of the illegal act. The amount of damages in health care terms is the amount paid for each false claim that is filed.

The Attorney General of the United States is required to diligently investigate violations of the FCA and may bring a civil action against a violator. The FCA also allows for private persons to bring actions for FCA violations *(qui tam* lawsuits). Individuals ("whistleblowers') who report fraud may be awarded a percentage of any monies recovered depending upon a number of factors, including, whether the government prosecutes the case, the factual bases, and/or the whistleblower's involvement in the act.

Generally, civil actions may not be brought more than six years after the violation, but in no event more than ten. When the action is filed, it is not disclosed (known as "under seal ") for at least sixty days. The U.S. Government may choose to intervene in the lawsuit and assume primary responsibility for prosecuting, dismissing or settling the action. If the Government chooses not to intervene, the private party who initiated the lawsuit has the right to conduct the action.

If the Government proceeds, the qui tam plaintiff may recover a portion of any proceeds of the action. If the *qui tam* plaintiff proceeds with the action without the government, the plaintiff may receive a larger portion of the recovery. In either case, the plaintiff may also receive an amount for reasonable expenses plus reasonable attorneys' fees and costs.

If the civil action is frivolous or brought primarily for harassment, the plaintiff may have to pay the defendant's fees and costs. If the plaintiff planned or initiated the violation, the share of proceeds may be reduced. If the plaintiff is found guilty of a crime associated with the violation, no share will be awarded to the plaintiff.

As addressed in Section 8 herein, the FCA provides protection for employees from retaliation. An employee who has been discharged, demoted, suspended, threatened, harassed, or in any way discriminated or retaliated against by his employer because of lawful acts conducted in furtherance of an action under the FCA is entitled to recover damages. Such damages include: reinstatement of employment status, two times the amount of back pay (plus interest), and compensation for any other damages the employee suffered as a result of the discrimination. The employee also can be awarded litigation costs and reasonable attorneys' fees.

2. **Program Fraud Civil Remedies Act; 31 U.S.C. §§ 3801 - 3812**

The Program Fraud and Civil Remedies Act ("PFCRA") creates administrative remedies for making false claims and false statements. These penalties are separate from and in addition to any liability that may be imposed under the FCA.

The PFCRA imposes liability on individuals or entities who file a claim that they know or have reason to know:

- Is false, fictitious, or fraudulent;
- Includes or is supported by any written statement that contains false, fictitious or fraudulent information;
- Includes or is suppor1ed by a written statement that omits a material fact, which causes the statement to be false, fictitious or fraudulent, and the person or entity submitting the statement has a duty to include the omitted fact; or
- Is for payment for property or services not provided as claimed.

Violations of this section of the PFCRA are punishable by a $5,500 civil penalty for each wrongfully filed claim, plus an assessment of twice the amount of any unlawful claim that has been paid.

In addition, a person or entity violates the PFCRA if they submit a written statement which they know or should know:

- Asserts a material fact that is false, fictitious or fraudulent; or
- Omits a material fact that they had a duty to include, the omission causes the statement to be false, fictitious or fraudulent, and the statement contained a certification of accuracy.

Violations of this section of the PFCRA are punishable by a civil penalty of up to $5,500 in addition to any other remedy allowed under other laws.

State False Claims Laws:

1. **Arkansas Medicaid Fraud Act; Ark. Code Ann. §§ 5-55-101** *et seq.*

The Arkansas Medicaid Fraud Act prohibits certain fraudulent actions taken "purposely" which means with a conscious intent to take the action or cause the result. Criminal liability is imposed for purposely taking any of the following actions:

- Making or causing to be made any false statement or representation of material fact in an application

for a Medicaid benefit or payment;

- Making or causing to be made any false statement or representation of material fact for use in determining rights to a Medicaid benefit or payment.
- Concealing or failing to disclose an event that intends to fraudulently secure the right to any Medicaid benefit or payment when no benefit or payment is authorized.
- Converting a Medicaid benefit or payment to another use after receiving it for the benefit of another person;
- Presenting or causing to be presented a claim for Medicaid payment for physician's services while knowing that the individual who furnished the services was not a licensed physician;
- Making or inducing the making of, any false statement or representation of a material fact with respect to the conditions or operation of any institution, facility or entity in order for that institution, facility or entity to qualify as a hospital, rural primary care hospital, skilled nursing facility, nursing facility, intermediate care facility for the mentally retarded, home health agency or other entity; or with respect to information required pursuant to applicable Federal and State law, rules, regulations and provider agreement;
- Charging rates for services to a Medicaid patient that are in excess of the rates established by the State;
- Charging, soliciting, accepting or receiving, in addition to the Medicaid payment, any consideration (other than a charitable, religious or philanthropic contribution) as a precondition of admitting a Medicaid patient to a facility or as a requirement for a Medicaid patient's continued stay in a facility;
- Making or causing to be made a false statement or representation of a material fact in any application for benefits or payment in violation of the Medicaid rules, regulations or provider agreements;
- Soliciting, receiving, offering or paying any remuneration in exchange for: (1) a referral for any item or service payable by Medicaid; or (2) the purchase, lease order or a recommendation to purchase, lease or order any good, facility, service or item payable by Medicaid. This provision does not apply to discounts that are properly disclosed and reflected in Medicaid charges or claims; payments under bona fide employment relationships; payments to purchasing agents pursuant to a written contract; or payments authorized under Arkansas Department of Health and Human Services ("DHHS") regulations.

Medicaid fraud is a Class B felony if the total amount of illegal payments is $2,500 or more and a Class C felony is the total amount is less than $2,500 but more than $200.

Penalties for a Class B felony may include imprisonment of not less than five (5) years, up to a maximum of twenty (20) years, and/or a fine of up to $15,000. Penalties for a Class C felony may include imprisonment of not less than three (3) years, up to a maximum of (1 0) years, and/or a fine of up to $10,000. If the total amount of illegal payments is less than $200, the offense is a Class A misdemeanor, which includes penalties of possible imprisonment of up to one (1) year and/or a fine of up to $1,000. The Medicaid Fraud Act also provides for additional criminal fines. Any person or entity found guilty of illegally receiving Medicaid funds is required to make full restitution to DHHS and pay a fine of three times the amount of the illegally received payments. A person or entity found guilty of fraudulently submitting Medicaid claims may be required to pay a fine of up to $3,000 for each fraudulent claim. Violators also may be suspended from participation in the Medicaid program.

The Arkansas Attorney General may pursue civil actions for Medicaid fraud. If a civil judgment is awarded on an Attorney General complaint alleging fraudulent receipt of Medicaid payments, the violating party must pay a civil penalty of two times the amount of all payments found to have been fraudulently received.

If a judgment is awarded for a complaint alleging fraudulent submission of Medicaid claims, a civil penalty of up to $2,000 for each fraudulently submitted claim may be imposed.

In either case, the violator may be required to reimburse the State for the expenses of enforcement. The

violator may also be suspended or terminated from the Medicaid program.

In Medicaid fraud cases, the court may award up to ten percent **(1**0%) of the total penalty recovered, but nor more than $100,000, to anyone who provided information that led to detecting and bringing to trial and punislm1ent persons guilty of violating the Medicaid Fraud Act.

2. **Arkansas Medicaid Fraud False Claims Act; Ark. Code Ann. §§ 20-77-901 *et** seq.*

The Arkansas Medicaid Fraud False Claims Act (the "Medicaid FCA") provides for civil penalties for knowingly engaging in the same activities that are prohibited under the Medicaid Fraud Act, plus either of the following activities:

- Participating, directly or indirectly, in the Medicaid program after pleading guilty or no contest to or being found guilty of Medicaid fraud, theft of public benefits or abuse of adults; or
- Employing, contracting or engaging an individual to participate in the business activities of a Medicaid provider when that individual has pleaded guilty or no contest to or has been found guilty of Medicaid fraud, theft of public benefits or abuse of adults.

"Knowingly" means that the person has actual knowledge of the information or acts in deliberate ignorance or reckless disregard of the truth or falsity of the information. Unlike the Medicaid Fraud Act, there is no requirement of a specific intent to defraud in order to impose liability under the Medicaid FCA.

Violators must make full restitution to the State, through the Attorney General, and pay a civil penalty of not less than $5,000 or more than $10,000 for each violation. They also must pay three times the amount of all payments fraudulently received, unless the party promptly disclosed the violation to the Attorney General's Office before any criminal, civil or administrative action had commenced, at the time of the disclosure the party had no knowledge of the existence of an investigation into the violation, and the party fully cooperated with the investigation. In the case of a prompt disclosure that meets the statutory requirements, the assessment may be reduced to two times the amount of fraudulent payments or less. Violators may be required to reimburse the State for the expenses of enforcement. Violators may also be suspended or terminated from the Medicaid program.

As under the Medicaid Fraud Act, the Medicaid FCA contains a provision that rewards those who report wrongdoing. Up to ten percent (10%) of the total penalty recovered, but not more than $100,000, may be awarded to anyone who provided information that led to detecting and bringing to trial and punishment those who violated the Medicaid FCA.

Role of False Claims Laws:

The false claims laws discussed above are an important part of preventing and detecting fraud and abuse in Federal and State health care programs because they provide governmental agencies the authority to seek out, investigate and prosecute fraudulent activities. Enforcement activities take place in the criminal, civil and administrative arenas. This provides a broad spectrum of remedies to battle these problems.

Individuals who observe activities or behavior that may violate the law in some manner and who report their observations either to management or to governmental agencies are provided protections under certain laws, such as the whistleblower protections under the FCA, listed above. These anti-retaliation protections for individuals who make good faith reports of fraud and abuse encourage reporting and provide broader opportunities to prosecute violators.

Policies and Procedures for Detecting and Preventing Fraud and Abuse:

WRHS has a compliance program, the primary purpose of which is to detect and prevent fraud, waste, and

abuse. WRHS's compliance program implements each of the seven primary elements established by the Federal Government, one of which is to provide an anonymous way by which employees may report suspected fraud, waste and abuse. This Policy is intended to provide guidance on how to resolve questions regarding legal and ethical issues, and to establish a mechanism for reporting possible violations of law or ethical principles within WRHS, including suspected fraud and abuse. Any questions concerning this Policy or the Program can be directed to the CO at (870)262-1481. WRHS has in place an anonymous hotline which employees and others may call and report suspected compliance violations toll free at 1(866)612-3136. In addition, the CO maintains an open-door policy to encourage employees to make these reports in person. All reports to the compliance hotline or the CO are investigated, and appropriate action is taken based upon the results of the investigation.

Any reports of actual or suspected violations may be made to the CO or to WRHS Administration. Reports will be kept confidential to the extent possible, consistent with the need to conduct an adequate investigation. Reports may also be made anonymously by anyone who files a complaint concerning a violation or suspected violation of any law, regulation, or WRHS policy. However, any allegations that prove not to be substantiated and which are proved to have been made with malicious intent or with knowledge of their falsity shall be considered a serious disciplinary offense.

WRHS expects all of its officers, administrators, employees, agents and contractors to comply with all applicable laws, regulations and WRHS policies and to report any concerns or complaints regarding violations or suspected violations. Failure to report suspected violations can result in disciplinary action.

The CO will investigate all reports of actual or suspected violations and take appropriate corrective action, if warranted. The CO has direct access to the Board of Directors and shall report on compliance activity at least annually. All reported concerns or complaints regarding corporate accounting practices, internal controls, or auditing shall be addressed by the Board of Directors or a Board committee, which shall report all findings and resolutions to the entire Board of Directors.

No member of the Board of Directors, administrator, officer, employee or agent who in good faith reports an actual or suspected violation of any law, regulation, or WRHS policy shall suffer harassment, retaliation or any adverse employment consequence. Any member of the Board of Directors, administrator, officer or employee who retaliates against someone who has made a good faith report pursuant to this Policy is subject to discipline, up to and including, termination of employment.

C. Record Retention Schedule

The retention periods contained in this document represent the *minimum* retention period that should be observed by all system employees.

Description	***Total Retention***
Compliance-Policies/Procedures	
Official company policies adopted by the COC	10 yrs
COC Minutes	
Includes meeting minutes, agendas and supporting documentation	Permanent
Compliance Audits-External	
Records reviewing and documenting ethics and compliance activities created as part of an audit conducted by an individual or group outside the organization. Includes executive summaries, audit reports, plans of corrective action, and audit work papers.	5 yrs

Compliance Audits-Internal

Copies of records reviewing documenting ethics and compliance activities created as part of an audit conducted by an Individual or group within the organization. Includes executive summaries, audit reports, plans of corrective action and audit work papers. 5 yrs

Compliance Investigation -Investigation Documentation

Records related to ethics and compliance investigations into alleged violations Including hot line complaints and other reports. Includes Investigation work papers, support and background documents and final reports. 10 yrs

Correspondence-General

Files containing copies of letters and memoranda sent to others and original letters and memoranda received from external sources/parties 3 yrs

Compliance-Correspondence with OIG

Files containing copies-reports, letters and memoranda sent to the Office of Inspector General and original letters and memoranda received from the Office of Inspector General 4 yrs

Compliance-Training Materials

Includes manuals, videotapes, guidebooks and supporting materials to train employees on ethics and compliance matters 4 yrs

Compliance- Communication Newsletters

Newsletters produced by the System 1yr

Compliance- CO Designation Forms

Forms designating CO Until Designee Is replaced

Compliance- General Quarterly Reports

Quarterly reports from Compliance Coordinators 4 yr

2. Compliance Officer and Compliance Oversight Committee

Overall responsibility for operation and oversight of the Compliance Plan belongs to the WRHS Board; however, the day-to-day responsibility for operation and oversight of the Compliance Plan rests first with the Compliance Coordinators of WRHS. The Compliance Coordinators report to the Compliance Oversight Committee (COC) on a quarterly basis. The COC is comprised of the Compliance Coordinators from various departments of the Corporation. The Compliance Officer (CO), who is appointed by the Board of Directors, serves as the liaison between the Compliance Oversight Committee and the Board of Directors.

Compliance Plan oversight will be provided by the CO and the COC. The CO and COC are vested with the authority to discharge their oversight responsibility as hereafter described:

A. The CO is responsible for the implementation, administration, and oversight of the COC. The CO is vested with the authority to carry out his/her duties according to the Compliance Plan policy statement.

B. The CO shall be responsible for the following duties:

1. Administer the Compliance Plan.
2. Encourage an awareness among corporation representative and the medical staff about compliance matters and the importance of adherence to the Standards of Practice.
3. Supervise monitoring, auditing, and reporting of activity within the scope of the Compliance Plan.
4. Establish a retribution-free system for reporting of noncompliance or concern about Compliance Plan matters.
5. Serve as ex officio member of the COC.
6. Routinely report results of monitoring, auditing, and reporting activity to the Board of Directors.
7. Provide leadership for the WRHS compliance effort.
8. With the assistance of in house counsel, retain the services of outside attorneys, accountants, consultants, and other professionals as needed.

C. The purpose of the COC is to oversee the implementation and operation of the Compliance Plan. The CO will review reports and recommendations of the COC regarding Compliance activities, including data regarding compliance generated through auditing, monitoring, and individual reporting. Based on these reports, the CO will make recommendations to WRHS Board of Directors regarding the efficacy of the Compliance Plan and will report as requested. The COC shall carry out other duties as described in the Compliance Plan.

1. The COC shall be composed of the CO or his/her designee, and a Compliance Coordinator from various departments of WRHS. A simple majority of the members present at a meeting shall constitute a quorum for voting purposes. In addition to the regularly scheduled meetings, the COC shall have the authority to call meetings as warranted by the situation.
    i. The COC shall meet at least quarterly at predetermined times and dates.
    ii. A summary of the items addressed and actions taken at each meeting shall be made and retained by CO or his/her designee.

2. The purpose and duties of the COC shall include, but are not limited to:
    i. Overseeing the implementation and operation of the Compliance Plan.
    ii. Receive and act upon reports and recommendations from the CO or high risk departments.
    iii. Evaluate the performance of the Compliance Plan and make recommendations accordingly.
    iv. Report actions and make recommendations to the appropriate WRHS officials.
    v. Performing other functions that may be reasonably necessary to fulfill the COC's responsibilities and purpose.
    vi. Become the authority on standards of conduct and legal risks associated with billing for professional services.
    vii. Develop policies and procedures for implementation and operation of the Compliance Plan.
    viii. Coordinate efforts by the Clinical Departments, Practice Groups, and Staff Services to implement the Compliance Plan.
    ix. Investigate possible noncompliance.
    x. Assist in the development of corrective action plans.

3. COC members are expected to regularly attend the scheduled and called COC meetings; however, absence may be excused by the CO for good cause. Chronic absenteeism (absence from two (2) consecutive meetings or three (3) meetings per year) without good cause shall be reported to the member's Administrative Representative, who will use the information in his/her yearly employee evaluation.

Any sensitive information regarding individuals or information identified as confidential or proprietary learned by a member during his/her tenure on the COC, shall be considered confidential, and the COC members shall not disclose such information unless otherwise directed by in house legal counsel.

4. At the CO's discretion, subcommittees may be formed from among the COC's membership to address specified issues.

3. Continuing Education and Training

All employees shall receive training on WRHS's Compliance Plan and Code of Conduct during new employee orientation, and refresher training shall be included in each employee's annual training program. Copies of the Compliance Plan and Code of Conduct will be made available to employees during training, and they will be encouraged to read those documents. The Compliance Plan and Code of Conduct will be published on the WRHS website and made available to employees by request at any time.

Those employees authorized to participate in WRHS's self study version of new employee orientation must submit a written certification verifying that they have been provided with a copy of the Compliance Plan, that they have read the Compliance Plan, and that they agree to be bound by and to comply with all aspects of the Compliance Plan.

All new employees shall submit a written certification that they agree to be bound by and to comply with all aspects of the Compliance Plan. In addition, all existing employees shall submit an annual written certification that they agree to be bound by and to comply with all aspects of the Compliance Plan.

All new employees shall return a signed acknowledgment card within thirty (30) calendar days of being hired. All existing employees shall submit an annual written certification that they agree to be bound by and to comply with all aspects of the Code of Conduct.

If an employee fails to receive Code of Conduct Training within thirty (30) calendar days of becoming a new employee, the employee must receive the training immediately. The reason the employee did not receive the training in a timely fashion, the name of the employee's supervisor, and an action plan for resolution must be reported to the CO.

Refresher training on the Code of Conduct shall be included in each employee's annual training program. Each Current Employee must receive Refresher Code of Conduct and Compliance Training each year. If any employee fails to receive Refresher Code of Conduct and Compliance Training by the end of the year, the employee must be immediately suspended without pay until such time as he/she receives the training.

An employee on leave at the end of the year who did not complete refresher training prior to taking leave, must receive the previous year's refresher training within thirty (30) calendar days of his/her return provided the current year's training has not been released.

If an employee returns after the current year's refresher training has been released, he/she will not need to receive the previous year's training and will only be required to receive the current year's training within thirty (30) calendar days of his or her return.

Certain employees from time to time are authorized to participate in a self study version of new employee orientation. All employees electing to do so will be provided with a copy of the Code of Conduct and complete an acknowledgment card verifying that they have read the Code of Conduct and agree to be bound by it.

4. Lines of Communication

A. Hotline

WRHS is committed to the timely identification and resolution of all issues that may adversely affect employees, patients, or the organization. Therefore, WRHS has established communication channels to report problems and concerns including a telephone hotline. The number for the Batesville area is (870) 612-3136 and the toll free line for employees outside the Batesville area is 1-866-612-3136. Employees are encouraged to report problems or concerns either anonymously or in confidence via the hotline when they deem appropriate. The hotline establishes an avenue for employees or interested parties to report suspected criminal activity and illegal or unethical conduct occurring within

WRHS in the event other resolution channels are ineffective or the caller wishes to remain anonymous.

A. WRHS will establish and maintain a telephone hotline that employees may use to report problems and concerns either anonymously or in confidence.
B. Employees who report problems and concerns in good faith via the hotline will be protected from any form of retaliation or retribution.
C. All those who are involved in the hotline operation are expected to act with utmost discretion and integrity, to assure that information received is acted upon in a reasonable and proper manner. Everyone who receives or is assigned responsibilities for hotline calls shall agree to the terms of confidentiality.
D. The CO is responsible for the daily operation of the employee hotline.
E. The CO's general responsibilities related to the hotline operation include addressing all hotline calls in an appropriate and timely manner, as well as in accordance with these and all related policies and procedures. Other responsibilities include the following:

    1. Monitoring proper functioning of the hotline;
    2. Establishing reporting and records maintenance procedures;
    3. Conducting appropriate investigations and follow-up;
    4. Referring calls when appropriate;
    5. Providing feedback to callers when necessary;
    6. Reporting hotline activity to the COC; and
    7. Maintaining security for all calls and related documents.

F. Qualified and properly trained personnel will answer and monitor the hotline.
G. All callers to the hotline will hear the same prerecorded message explaining their rights, any limitations, the non-retaliation policy, and other pertinent information.
H. No attempt will be made to identify a caller who requests anonymity.
I. Whenever callers disclose their identity, it will be held in confidence to the fullest extent practical or allowed by law.
J. The CO, or their designee, will communicate any matter deemed potentially unlawful to in house legal counsel.
K. Calls will be documented on the White River Health System Compliance Issue Log. All call records will be logged and sequentially numbered upon receipt on this form and placed in the care and custody of the CO, or his or her designee.
L. When a hotline call is received, the caller should be asked to call back at a designated date and time to provide additional information or notify the caller of resolution.
M. The hotline operation will involve other departments, as appropriate, for advice or further investigation. In the event that the CO is not, in good faith, satisfied that a matter brought before the aforesaid departments was appropriately addressed and resolved, the CO will be responsible for and is authorized to take the matter to other persons in positions of authority.

The CO will report periodically to the Board of Directors regarding hotline activity. This report will include the total number of calls received, acted upon, and general results from the hotline operation. In addition, the report will include any recommendations for system-wide improvements or corrective actions arising from the results of the operation and related investigations.

B. Whistleblower Policy

It is the responsibility of all members of the Board of Directors, administrators, officers, and employees of WRHS to observe the highest standards of business and personal ethics in the conduct of their duties and responsibilities at WRHS as reflected in our Code of Conduct. All members of the Board of Directors, administrators, officers, and employees of WRHS are expected to comply with all applicable laws and practice honesty and integrity in fulfilling their responsibilities to WRHS.

All members of the Board of Directors, administrators, officers, and employees of WRHS are expected and

encouraged to report any concerns or complaints regarding violations or suspected violations of the Code of Conduct. No member of the Board of Directors, administrator, officer, or employee, who in good faith reports a violation of the Code of Conduct shall suffer harassment, retaliation, or any adverse employment consequence. An employee who retaliates against someone who has reported a violation in good faith is subject to discipline, up to and including, termination of employment.

Suspected violations may be reported to an individual's immediate supervisor. If the individual is not comfortable speaking with his or her supervisor, or if the individual is not satisfied with the supervisor's response, he or she is encouraged to speak with someone in the Human Resources Department or anyone In Hospital Administration.

Supervisors and managers are required to report suspected violations of the Code of Conduct to the CO, who has specific and exclusive responsibility to investigate all reported violations. For suspected fraud, or when an individual is not satisfied or uncomfortable with following the organization's open door policy, individuals should contact the CO directly.

The CO is responsible for investigating and resolving all reported complaints and allegations concerning violations of the Code of Conduct and, at his or her discretion, shall advise the Chief Executive Officer and/or the Board of Directors. The CO has direct access to the Board of Directors and is required to report on compliance activity at least annually.

All reported concerns or complaints regarding corporate accounting practices, internal controls, or auditing shall be addressed by the Board of Directors or a committee that the Board has delegated this duty, which shall report to the Board all findings and resolutions.

Anyone who files a complaint concerning a violation or suspected violation of the Code of Conduct must act in good faith and have reasonable grounds for believing the information reported indicates a violation of the Code of Conduct. Any allegations that prove not to be substantiated and which are proved to have been made with malicious intent or with knowledge of their falsity shall be considered a serious disciplinary offense.

Violations or suspected violations may be submitted on a confidential basis by the complainant or may be submitted anonymously. Reports of violations or suspected violations shall be kept confidential to the greatest extent possible, consistent with the need to conduct an adequate investigation.

All reported concerns or complaints shall be promptly Investigated by the CO, and appropriate corrective action shall be taken if warranted by the investigation.

5. Enforcement

WRHS shall enforce its prohibition against employment of ineligible persons. For purposes of this policy, an "Ineligible Person" shall be any individual or entity who:

i. is currently excluded, suspended, debarred or otherwise ineligible to participate in any Federal or State healthcare programs;

ii. has been convicted of a criminal offense related to the provision of healthcare items or services and has not been reinstated in the Federal or State healthcare programs after a period of exclusion, suspension, debarment, or ineligibility; or

iii. is currently listed on a state exclusion list.

No System facility, including hospitals, ambulatory surgery centers, home health agencies, and physician practices will make an offer of employment to an applicant who is listed as an Ineligible Person.

All applicants are required to answer the following questions on the application for employment: Are you currently excluded, suspended, debarred or otherwise ineligible to participate in any Federal or State healthcare programs, or have you been convicted of a criminal offense related to the provision of healthcare items or services but not yet been excluded, debarred or otherwise declared ineligible?

Each employee of a System facility must disclose immediately any debarment, exclusion *or* other event that makes him *or* her Ineligible Person.

All System facilities, including hospitals, home health agencies, and physician practices must immediately terminate any current employee who is listed as an Ineligible Person.

i. Prior to hiring or re-hiring an employee, Human Resources must check each individual being considered for employment against the General Service Administration's List of Parties Excluded from Federal Programs (the "GSA List") and the HHS/OIG List of Excluded Individuals/Entitles (the "OIG" Sanction Report"), the Arkansas Medicaid Sanctioned Provider list and the Arkansas DF&A De-barred List (collectively the "Lists").
ii. Human Resources will compare the name and address of each potential candidate for employment to the Lists. Should an individual appear on the Lists, WRHS may not employ that individual until the charges are resolved and it is clear that the individual has not been excluded or debarred. Should an individual submit an affidavit that he/she is not the individual that appears on any of the Lists, that individual may be considered eligible for employment.
iii. The Human Resources Department will compare WRHS's employee database against the Lists on a monthly basis (for the Arkansas Medicaid Sanctioned Provider List and the Arkansas DF&A De-barred list) and annually (for the GSA List and the OIG Sanction Report) and provide the report of the comparison, which lists potential matches, to the Director of that particular WRHS department.
iv. The Director, or designee, Is responsible for confirming the match, and if the employee is an Ineligible Person on any of the Lists, the Human Resources Director must terminate the employment relationship with that individual. The Human Resources Director will report the match and the action taken by the facility to the COC.

Each employee must immediately disclose to his or her supervisor any debarment, exclusion or other event that makes the employee an Ineligible Person. The supervisor must report such disclosures to the Director, and the Human Resources Director must terminate the employment relationship with that individual.

6. Monitoring and Auditing

A. Risk Assessment, Monitoring, and Investigation

Annual Risk Assessment and Compliance Work Plan.

Development of Risk Assessment and Compliance Work Plan - The CO is responsible for coordinating an annual written risk assessment of identified risk areas for compliance with federal and state laws and regulations. The objective of the annual risk assessment is to identify and prioritize actual or potential areas presenting compliance concerns and to recommend measures to address such concerns. The CO is responsible for developing, implementing and, as appropriate, modifying the procedure for performing the annual risk assessment. Taking the results of the annual risk assessment into consideration, the CO will develop an annual compliance work plan, which shall include requirements for training on and monitoring of areas identified as high risk.

Resources - The CO will work in a cooperative effort with individual departments, the COC, and other key management personnel to complete the annual risk assessment and annual compliance work plan. If responsibility for particular aspects of the annual risk assessment is delegated by the CO to individual departments, committees or

management personnel, the designated party or parties will prepare and submit reports documenting the results of the annual risk assessment to the CO. The results of the risk assessment may be verified by internal or external audits, consultants or such other means as the CO determines to be necessary and appropriate. The CO will assist in resolving any compliance issues by engaging in, as appropriate, internal compliance monitoring, establishment or enhancement of internal controls, development or revision of applicable policies, additional compliance training or other appropriate means to maintain compliant operations.

Investigation - The CO, in conjunction with in house legal counsel, is responsible for directing Compliance investigations and may solicit the support of internal and external resources to conduct the investigation. Investigations shall be carried out in accordance with the Compliance Officer Protocol and Procedures.

Reporting - The CO shall provide a written report of the findings of the annual risk assessment and annual compliance work plan to the COC, which shall in turn make a report to the Board of Directors for review. The annual report shall identify actual or potential areas of concern, a description of current measures taken and recommendations to address areas of concern. The annual compliance work plan shall include requirements for training on and monitoring of areas identified as high risk. The annual compliance work plan shall be approved by the COC.

Risk Areas.

The annual risk assessment shall give special emphasis to risk areas associated with billing practices, and shall include a review of other actual or potential risk areas identified through internal or external audits; in the Office of Inspector General's ("OIG") annual Work Plan, Fraud Alerts, or other published compliance guidance; or otherwise by the CO or COC. The list of risk areas below is a compilation of potential risk areas that may be subject to the annual risk assessment, as determined to be appropriate by the CO or COC. This list is not meant to be exhaustive, and other areas of risk may be identified and assessed as deemed necessary by the CO, the COC, the Board of Directors, managers or supervisors.

i. *Billing and Coding Practices* - Includes a review of cost reports, billing and coding practices (including whether adequate documentation exists to support the medical necessity of the services and supplies provided), the costs charged and the submission of proper insurance claims. The individuals involved in each step of the billing process shall also be identified. The CO shall report the results to the COC.

ii. *Business Conduct and Practices* - Includes identification of the individuals with authority to enter into contractual relationships and examines how vendors and suppliers are chosen. Adherence to conflict of interest policies may also be assessed to ensure that conflicts are properly disclosed and managed. The CO, or his/her designee, shall perform this assessment.

iii. *Human Resources* - Includes a review of the hiring process to ensure that clinical personnel are properly licensed and that new hires do not have previous health care related convictions and are not excluded from participation in federal health care programs. Employee job descriptions and performance evaluations shall be reviewed to ensure incorporation of compliance expectations and responsibilities, including adherence to the Compliance Plan and the Code of Conduct. Disciplinary actions and terminations of Employees who have been determined to have engaged in improper activity shall also be reviewed to identify any actual or potential violation of state, federal, or local laws or regulations. Human Resources shall perform this assessment and report the results to the CO.

iv. *Medicare/Medicaid Referral, Fraud and Abuse, and False Claims Prohibitions* - Includes a review of contracts with physicians, physician-owned entities and other health care providers to monitor that appropriate business arrangements are in effect that do not include improper referrals or a relationship with a party that has previous health care convictions or is otherwise excluded from

participation in the federal health care programs. The CO, or his/her designee, shall perform this assessment.

vi. *Risk Management* - Includes a review of applicable policies and procedures that exist for patient and employee safety, and assessing compliance with articulated policies and procedures. The CO shall cooperate with the Director of Risk Management or other appropriate senior leader(s) to perform this assessment.

vii. *Compliance with Medicare Conditions of Participation* - Includes an assessment of compliance with Medicare and Medicaid conditions of participation, which may involve an examination of previous survey findings. The CO, or his/ her designee, shall perform this assessment.

viii. *Quality of Care* - Includes an evaluation of quality control capabilities and potential exposure to quality of care compliance issues to maintain levels of care that are consistent with generally accepted standards of health care. Such assessment may include a review of the following: policies and procedures related to quality care, training provided on quality issues, reporting of quality concerns, and whether the CO is timely informed of quality concerns so that any impact on billing and payment may be evaluated. The Chief Medical Officer shall perform this assessment and report the results to the CO.

ix. *EMTALA* - Includes a review of compliance with the Emergency Medical Treatment and Labor Act of 1986 ("EMTALA") and its implementing regulations, which require the evaluation, admission, and treatment of patients with emergency medical conditions and pregnant women who are in labor. The Chief Clinical Officer (CCO) shall perform this assessment and report the results to the CO.

x. *Tax-Exemption* - Includes a review of operating practices to maintain compliance with section 501(c)(3) of the Internal Revenue Code and, as appropriate, property tax exemption requirements. The CO, or his or her designee, shall perform this assessment.

xi. *Privacy and Security* - Includes a review of privacy and security policies and practices that have been adopted in compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH") and with other federal and state laws mandating the confidentiality and security of, as well as access to, patient health information. The CO and the Chief Quality Officer shall cooperate to perform this assessment.

B. External Audit Firm

The following guidelines and rules are to be followed by WRHS in formulating and carrying out its relationship with WRHS's external audit firm.

Selection of Audit Firm

1. On a triennial basis, WRHS will issue a request for proposal from between three and five audit firms who are independent, reputable, and experienced in hospital auditing. The Audit Committee will review all bids and select the audit firm based on cost and quality of service. The Audit Committee recommendation will be forwarded to the WRHS Board of Directors for final approval.
2. Any audit firm submitting a bid for services must meet any specific audit firm requirements as set forth in WRHS bond documents. These requirements, if any, will be listed in the request for proposal.
3. For the second and third year of the auditor engagement, the Audit Committee will review and approve the audit bid based on scope of services, complexity of organization and inflation.

Responsibility of Audit Firm - The audit firm will be hired by and report to the Audit Committee of the WRHS Board of Directors.

Pre-Approval of Services - The Audit Committee will pre-approve all services, both audit and non-audit, to be provided by the audit firm.

Audit Reporting Requirements - The audit firm will provide the WRHS Board of Directors the following items:

1. An annual audit presented in a form acceptable per GAAP.
2. A report listing certain supplementary financial information in a format acceptable to the Audit Committee.
3. A management letter which details areas of concern in the System's internal control structure.
4. A letter detailing all reportable conflicts of interest at WRHS, as well as the audit firm's analysis and conclusions regarding conflicts of interest.
5. A letter detailing WRHS compliance with all outstanding bond indenture requirements.
6. Provide, by separate letter, a listing of fees paid to the audit firm for audit services and any other services provided to WRHS.

Communication with Audit Committee - Prior to the audit firm's submission of the final audit report to the WRHS Board of Directors, the audit firm will meet with the Audit Committee, without management, and present the following:

1. The preliminary, draft audit report.
2. A list of all audit adjustments made to the books and records by the audit firm and an explanation of each.
3. All critical accounting policies and practices used by WRHS.
4. All material alternative accounting treatments of financial information within GAAP that have been discussed with management, including the ramifications of the use of such alternative treatments and disclosures and the treatment preferred by the audit firm.
5. All material written communications between the audit firm and management of WRHS.

Non-Audit Services - With the exception of providing information related to tax return and Medicare/Medicaid cost report preparation, the audit firm will not provide WRHS any non-audit services without prior WRHS Audit Committee approval. In order for these non-audit services to be pre-approved by the WRHS Audit Committee, it must be demonstrated that the provision of such services, in addition to the annual audit services, will not impair the independence of the audit firm.

Other Independence Rules - The audit firm would not be deemed to be independent if (1) any members of the WRHS management team had been employed by the audit firm within a one-year period immediately preceding the commencement of audit procedures or (2) any audit firm's partners received compensation based on the partner's procuring engagements with WRHS for services other than audit, review and attest services.

7. Detection, Investigation & Response to Offenses

A. Compliance Issue Resolution

WRHS implemented a Compliance Plan in an effort to establish a culture within the organization that promotes prevention, detection, and resolution of misconduct, fraud, or abuse. This is accomplished, in part, by establishing communication channels for employees to report problems and concerns. Employees are encouraged to report issues via the traditional chain of command, human resources, employee hotline, or directly to the CO. Therefore, the CO is responsible for responding to employee issues that are raised through the various communication channels. This policy is designed to establish a framework for managing and responding to compliance issues that are raised to the CO.

Policy

1. Employees are allowed to use any communication channel they deem appropriate to report issues.
2. Retaliation or retribution for reporting issues in good faith is prohibited.
3. The CO is only responsible for resolving compliance-related issues; however, employees should not be discouraged from using any specific communication channel. Rather, employees should be politely redirected or the CO should redirect noncompliance-related issues to the appropriate department or individual.
4. The CO is responsible for the compliance program; therefore, issues related to the operation of the program should be referred to the CO or the COC. To the extent practical or allowed by law, the CO must maintain the confidentiality or anonymity of an employee when requested.

Procedures

1. Employee hotline calls will be handled In accordance with established policies and procedures.
2. Issues received by the CO or COC will be either referred to the appropriate department or individual or responded to within 30 days.
3. Issues with the potential for legal liability or containing issues of a legal nature will be referred to in house legal counsel.
4. The CO should involve various members of the management and employee population when appropriate to resolve issues.
5. For compliance related issues, the CO , COC or their designee, will conduct an initial inquiry that may Include document review, interviews, audit, or other investigative technique. The CO or COC, should: (a) conduct a fair impartial review of all relevant facts; (b) restrict the inquiry to those necessary to resolve the issues; and (c) conduct the inquiry with as little visibility as possible while gathering pertinent facts relating to the Issue.
6. The CO should ensure that the following objectives are accomplished:
   - Fully debrief complainant;
   - Notify appropriate internal parties;
   - Identify cause of problem, desired outcome, affected parties, applicable guidelines, possible regulatory or financial impact;
   - Provide a complete list of findings and recommendations;
   - Determine the necessary corrective action measures (e.g., policy changes, operational changes, system changes, personnel changes, training/education);
   - Document the inquiry.

   All inquiry records should be maintained in accordance with WRHS's policies for record retention.

B. Compliance Officer Protocol and Procedures

One of the primary purposes of the Compliance Plan is to identify any misconduct that might constitute a violation of criminal, civil, or administrative law. Therefore, it is necessary to establish protocols and procedures to guide the activities of the CO.

1. Upon report or notice of suspected noncompliance with any criminal, civil, or administrative law, the CO will conduct an "initial inquiry" into the alleged misconduct. The purpose of the initial Inquiry is to determine whether there is sufficient evidence of possible noncompliance to warrant further investigation.
2. If, during the initial inquiry, the CO determines that there is sufficient evidence of possible noncompliance to warrant further investigation, the CO shall contact in house legal counsel, for direction on proceeding with the investigation.
3. Upon reasonable evidence of suspected noncompliance with any criminal, civil, or administrative law, in house legal counsel should conduct an investigation into the legal sufficiency of the allegations.
4. In light of timely reporting requirements, credible allegations of misconduct related to billing and reimbursement should be turned over to in house legal counsel as expeditiously as possible.
5. During any investigation, in house legal counsel and the CO must ensure that all relevant evidence is

preserved.

6. If WRHS wants documents produced during the investigation by in house legal counsel to be protected from disclosure, all such documents should include the statement: "Privileged and Confidential Document: Subject to Attorney-Client Privileges: Attorney Directed Work Product."
7. In house legal counsel will conduct an investigation to evaluate the facts to determine whether credible evidence exists to indicate that a violation of criminal, civil, or administrative law has occurred. It will also be the responsibility of in house legal counsel to:
   i. Notify the CEO and the CO of the organization of the results of its legal investigation; and
   ii. Provide sufficient factual details from its legal investigation to allow the CO to properly address any compliance issue.

Both the initial inquiry and legal investigation will be conducted as expeditiously as possible.

C. Correction of Errors Related to Billing for Healthcare Services

WRHS has implemented a policy to help assure that all WRHS employees and staff comply with WRHS billing, documentation, and coding policies and procedures, and billing requirements of federal and state agencies and third-party payers, and to establish a method to identify and correct errors and return any overpayments received by WRHS.

For purposes of this section, "Federal healthcare program" means: Any plan or program that provides health benefits, whether directly, through insurance, or otherwise, which is funded directly, in whole or in part, by the United States Government or any State health care program, as defined in 42 U.S.C. 1320a-7(h}.

Federal healthcare programs include, at a minimum, the following:

- Medicare Program, Parts A & B;
- Medicaid (Title XIX of the Social Security Act);
- Federal Prison Hospitals (prisoners);
- Indian Health Service;
- Medicare Advantage Plans;
- OWCP (workers' compensation for federal employees);
- Railroad Retirement Board;
- The Black Lung Program;
- TRICARE/CHAMPUS/Department of Defense healthcare programs;
- Veterans Administration (VA}; and
- Federal Employee Health Benefits Plan (FEHBP).

A. All appropriate employees and staff members will receive periodic training on this policy and WRHS billing and coding procedures.
B. Claims for healthcare services provided by WRHS will be submitted based on supporting documentation and In compliance with state and federal laws and regulations and applicable policies.
C. Fraudulent behavior or willful misconduct (such as falsifying documentation for billing purposes) will not be tolerated. Any employee or staff member engaging in such non-compliant behavior will be subject to disciplinary action, up to and including termination of employment or staff privileges.
D. Anyone with knowledge of a potential error in billing, coding, or reimbursement error or possible misconduct related to billing for healthcare services must provide to the appropriate WRHS manager all information related to the potential error or misconduct with as much specificity as possible regarding the type of occurrence, including the date and the dollar amount involved, if known.
E. Routine processing errors should be corrected by either the individual who detects the error or the person who committed the error. Such errors should also be reported to a supervisor.
F. Reports of credit balances will be reported to the COC on a quarterly basis.

G. After receipt of information related to a potential error or misconduct, the WRHS manager, in consultation with facility leadership, will take whatever steps are necessary to determine whether the alleged incident occurred, including investigating the particular situation and seeking to determine whether the matter is isolated in nature or part of a pattern.
H. WRHS will report to the appropriate agency or third party payer any confirmed healthcare program reimbursement errors that have resulted in overpayment to WRHS and return any such overpayments within 60 days of discovery through rebilling, refund, or other appropriate means. Program errors involving underpayments will also be reported to the appropriate party.
I. Remedial action to correct the cause of the overpayment and to decrease the likelihood of its recurrence must occur within 60 days of the overpayment confirmation.
J. Internal audits will be performed periodically to monitor compliance with WRHS policies and procedures related to billing for health care services to identify and correct deficiencies. Reports of such audits will be reported to the COC.
K. External audits by independent consultants may also be performed periodically. Any deficiencies discovered will be corrected, and applicable employees and staff will receive appropriate education and training to prevent recurrence of such deficiency.
L. Upon discovery of credible evidence that misconduct has occurred which may be a violation of law, WRHS will promptly self-report the discovery to the appropriate state or federal authorities within 60 days of discovery. WRHS will also fully cooperate with authorities to correct and remedy the problem.

8. Miscellaneous Policies and Procedures

A. Identity Theft Prevention Policy

To assist in the detection and prevention of identity theft in accordance with the Fair and Accurate Credit Transactions Act ("FACT Act"), all WRHS staff who work with Covered Accounts or personal or protected health information ("PHI") of patients for treatment, payment, or operations shall comply with this policy.

1. Covered Account: Refers to (a) any account offered or maintained primarily for personal, family or household purposes, which involves multiple payments or transactions, including one or more deferred payments; or (b) any other account identified as having a reasonably foreseeable risk of identity theft to customers or to the safety and soundness of the Hospital. For purposes of this policy, "Covered Account" will include, without limitation, any account which contains personal information that can be used to gain access to a person's identity for financial or healthcare purposes.

2. Identity Theft: Refers to fraud committed or attempted through the use of identifying information of another person.

3. Notice of Address Discrepancy: A notice sent by a consumer reporting agency ("CRA") that informs WRHS of a difference between the patient address that WRHS provided to request a consumer report and the address(es) on file at the CRA.

4. Personal Information: Social security number, driver's license number, alien registration number, government passport number, financial account number, credit card number, employer or taxpayer identification number, personal identification numbers, mother's maiden names, passwords, and any other unique identification number or piece of key information that can be used to gain access to a person's financial resources, or to assume a person's identity.

5. Red Flag: A pattern, practice, or specific activity that indicates the possible existence of identity theft. Examples include:

i. Presentation of suspicious or altered documents;
ii. Presentation of suspicious, inconsistent, or altered personal identifying information such as an identification card that is inconsistent with patient's appearance or a suspicious address;
iii. Repeated failure or refusal to provide identifying information;
iv. Presentation of personal identifying information that is associated with known fraud activity;
v. Presentation of a social security number that matches one submitted by another patient or differs from one submitted on a prior visit;
vi. Inability to verify insurance information;
vii. Family members or friends reveal suspicious information to WRHS staff, such as calling the patient by a different name;
viii. The patient provides information in the medical consultation that is inconsistent with the medical history;
ix. Allegations from an individual that his/her identity has been stolen, or that services billed were not received by that individual;
x. Mail sent to the patient is repeatedly returned as undeliverable despite ongoing transactions;
xi. Alerts, notifications, or other warnings received from a CRA or service providers, such as a fraud alert, active duty alert, or a notice of credit freeze;
xii. Notices from patients, victims of identity theft, law enforcement, or other persons regarding possible identity theft in connection with patient accounts;
xiii. Notice that WRHS has opened a fraudulent account for a person engaged in identity theft;
xiv. Notice of an address discrepancy from a consumer repm1ing agency;
xv. Notice from a consumer reporting agency of a pattern of activity that is inconsistent with the patient's hi story and usual pattern of activity; or
xvi. Attempts to access an account by unauthorized users.

All WRHS staff members are responsible for promptly notifying their direct supervisor of any circumstance that arises with a patient or patient's family that creates doubt or suspicion regarding the integrity and accuracy of the information provided by the patient. Department management is responsible for communicating the detection of the Red Flag to the CO.

Identification and Detection of Red Flags - All WRHS staff who register/schedule patients will take reasonable action to identify and detect relevant red flags.

1. *Identifying Information:* When registering or scheduling a new patient, WRHS staff will collect the patient's name, gender, date of birth, address, and identification number from the patient or the patient's representative. Examples of identification numbers include: a social security number, taxpayer identification number; passport number, or any other government-issued identification number.

2. *Identity Verification:* When registering or scheduling an established patient, WRHS staff will compare information provided by the patient or the patient's representative with information contained in the database to identify discrepancies.

3. *Identity Authentication:* For all patients, new or established, WRHS staff shall verify the identity of the patient or the patient's legal representative, by requesting to view a photo identification of the patient or the patient's representative, along with their insurance card, or by other reasonable means.

Exception: A patient will never be denied emergency medical care because the patient or the patient's representative is unable to provide identifying information at the time of registration or scheduling.

Response to Red Flags:

1. *Notification* - Any time an employee is faced with a "Red Flag" situation, the employee's direct supervisor or the CO shall be notified.

2. *Documentation* - All detected Red Flags shall be documented. Such documentation shall include all identifying information about the individual; a description of any document that was relied upon to verify the identifying information; a description of any additional measures undertaken to verify the identity of the individual and a description of any substantive discrepancy discovered when verifying the individual's identifying information.

3. *Response* - The CO will investigate each detected Red Flag. Reponses to Red Flags will depend on the results of the investigation and may include:

    i. Contacting the patient;
    ii. Notifying law enforcement;
    iii. Correcting the medical record;
    iv. Correcting the account to ensure accuracy;
    v. Placing the Covered Account on hold until the Red Flag is resolved
    vi. Updating or enhancing computer security;
    vii. Changing passwords or security codes; or
    viii. Determining that no action is warranted under the circumstances.

    In the event of a security breach involving unauthorized access of computerized data containing personal information of patients, affected individuals shall be notified as required by law in the most expedient time and manner possible without unreasonable delay, consistent with the needs of law enforcement.

4. *Response to Address Discrepancies* - In the event that a Notice of Address Discrepancy is received from a CRA, WRHS will make a reasonable attempt to verify the correct address. The CRA will be notified if the address is verified as correct. If address verification cannot be obtained within a reasonable time period, the account will either be closed or placed on hold until address verification is obtained.

5. *Mitigation* - In the event that an investigation reveals a reasonable belief that identity theft has occurred, WRHS will attempt to mitigate the identity theft to the greatest extent possible.

6. In addition to notifying law enforcement, the patient or his or her representative will be provided with information regarding the scope of the breach, the information accessed, how the information was used, if known, the actions taken to remedy the situation, and the contact information of CO. In addition, the patient will be directed to the http://www.gotyourbackarkansas.org *(Arkansas Attorney General information attached as Appendix B for more on identity theft).*

7. If Medicare or Medicaid fraud is discovered (where a patient uses another person's Medicare or Medicaid information to obtain medical care), the fraud will be reported to the Office of the Inspector General and/or the Medicaid office, as applicable.

8. Accounts affected by actual or suspected identity theft will be placed on hold until all medical and billing records have been corrected.

Administration and Oversight

1. *Ongoing Monitoring* - This policy and procedure will be administered and monitored by the CO.

2. Documentation and Records Retention - *All documentation concerning actual or suspected identity theft will* be maintained by the CO. Documentation of each investigation will a description of the identifying information and the method used for verification; a description of discrepancies discovered; and the actions taken as a result of the investigation. This documentation will be maintained for a period of five (5) years

after the account is closed or becomes dormant. Following the required time period for document retention, the records will be disposed of in a manner to protect against unauthorized access or use of the information contained in the records.

3. *Accounting for Disclosures* - If an investigation reveals that protected health information was inappropriately disclosed, such disclosure will be accounted for in accordance with the WRHS HIPAA Privacy and Security policies.

4. *Service Providers* - All service providers who contract with WRHS to perform activities in connection with patient accounts will (i) implement policies and procedures to detect relevant Red Flags that may arise during the performance of such activities; (ii) promptly notify WRHS of any relevant Red Flags that may arise during the performance of such activities; and (iii) take appropriate steps to prevent and mitigate identity theft.

5. *Risk Assessment* - An annual risk assessment will be conducted to determine which business accounts pose a risk of identity theft to patients. This risk assessment will take into consideration (i) the methods used to open accounts; (ii) the methods used to access accounts; and (iii) any prior experiences with identity theft. Any business accounts that pose a reasonably foreseeable risk of identity theft to patients will become subject to the provisions of this Policy.

6. *Education* - All employees who work with Covered Accounts or PHI for treatment, payment, or operations will receive annual education and training on the prevention of identity theft.

7. *Compliance Reports* - Compliance reports which detail any incidents of identity theft and the responses implemented, as well as recommendations concerning this Policy, will be provided to the Board annually.

8. *Program Review* - This Program will be reviewed and updated annually in response to (i) any experiences WRHS has with identity theft; (ii) changes in methods of identity theft experienced by the industry; changes in methods to detect, prevent, and mitigate identity theft; (iii) changes in the types of accounts offered or maintained; or (iv) any changes in the business arrangements, including mergers, acquisitions, joint ventures, and service provider arrangements.

B. Conflict of Interest

Purpose

The purpose of the conflicts of interest policy is to protect the WRHS's interest when it is contemplating entering into a transaction or arrangement that might benefit the private interest of a member of the Board of Directors, administrator, officer, or manager of WRHS. The policy is intended to supplement but not replace any applicable state laws governing conflicts of interest applicable to nonprofit and charitable corporations.

Definitions

1. Interested Person - Any member of the Board of Directors, administrator, manager, or member of a committee with Board delegated powers, when such administrator, manager, or member has a direct or indirect financial interest, as defined below, is an interested person. If a person is an interested person with respect to any entity in WRHS, he or she is an interested person with respect to all entities in WRHS.
2. Financial lnterest - A person has a financial interest if the person has, directly or indirectly, through business, investment or family:
    i. an ownership or investment Interest In any entity with which WRHS has a transaction or arrangement, or

ii. a compensation arrangement with WRHS or with any entity or individual with which WRHS has a transaction or arrangement, or
iii. a potential ownership or investment interest in, or compensation arrangement with, any entity or individual with which WRHS is negotiating a transaction or arrangement.

A financial interest is not necessarily a conflict of interest. A person who has a financial interest has a conflict of interest only if the appropriate board or committee decides that a conflict of interest exists.

3. Compensation – That which includes direct and indirect remuneration as well as gifts or favors that exceed $5,000 per annum.

Procedures

1. *Duty to Disclose* - In connection with any actual or possible conflicts of Interest, an interested person must disclose the existence of his or her financial interest and all material facts to the directors and members of committees with board delegated powers considering the proposed transaction or arrangement.

2. *Determining Whether a Conflict of Interest Exists* - After disclosure of the financial interest and all material facts, and after any discussion with the interested person, he or she shall leave the Board or committee meeting while the determination of a conflict of interest is discussed and voted upon. The remaining Board of Directors or committee members shall decide if a conflict of Interest exists.

3. Procedures for Addressing the Conflict of Interest:

i. An interested person may make a presentation at the Board or committee meeting, but after such presentation, the person shall leave the meeting during the discussion of, and the vote on, the transaction or arrangement that results in the conflict of interest.

ii. The Chairperson of the Board or committee shall, if appropriate, appoint a disinterested person or committee to investigate alternatives to the proposed transaction or arrangement.

iii. After exercising due diligence, the Board or committee shall determine whether WRHS can obtain a more advantageous transaction or arrangement with reasonable efforts from a person or entity that would not give rise to a conflict of interest.

iv. If a more advantageous transaction or arrangement is not reasonably attainable under circumstances that would not give rise to a conflict of interest, the Board or committee shall determine by a majority vote of the disinterested Directors or members whether the transaction or arrangement is in WRHS's best interest and for its own benefit and whether the transaction Is fair and reasonable to WRHS and shall make its decision as to whether to enter into the transaction or arrangement in conformity with such determination.

4. Violations of the Conflicts of Interest Policy

i. If the Board or committee has reasonable cause to believe that an Interested Person has failed to disclose actual or possible conflicts of interest, it shall inform the Interested Person of the basis for such belief and afford the Interested Person an opportunity to explain the alleged failure to disclose.
ii. If, after hearing the response of Interested Person and making such further investigation as may be warranted in the circumstances, the Board or committee determines that the Interested Person has in fact failed to disclose an actual or possible conflict of interest, it shall take appropriate disciplinary and corrective action.
iii.

Records of Proceedings

The minutes of the Board and all committees with board-delegated powers shall contain:

1. The names of the persons who disclosed or otherwise were found to have a financial interest in connection with an actual or possible conflict of interest, the nature of the financial interest, any action taken to determine whether a conflict of interest was present, and the board's or committee's decision as to whether a conflict of interest in fact existed.
2. The names of the persons who were present for discussions and votes relating to the transaction or arrangement, the content of the discussion, including any alternatives to the proposed transaction or arrangement, and a record of any votes taken in connection therewith.

Compensation Committees

1. A voting member of any committee whose jurisdiction includes compensation matters and who receives compensation, directly or indirectly, from WRHS for services is precluded from voting on matters pertaining to that member's compensation.
2. Physicians who receive compensation, directly or indirectly, from WRHS, whether as employees or independent contractors, are precluded from membership on any committee whose jurisdiction includes compensation matters. No physician, either individually or collectively, is prohibited from providing information to any committee regarding physician compensation.

Periodic Reviews and Annual Statements

1. To maintain WRHS operations in a manner consistent with its charitable purposes and to monitor WRHS does not engage in activities that could jeopardize its status as an organization exempt from federal income tax, periodic reviews shall be conducted and reported to the Finance Committee.
2. The periodic reviews shall, at a minimum, include the following subjects:
    i. Whether compensation arrangements and benefits are reasonable and are the result of arm's-length bargaining;
    ii. Whether acquisitions of physician practices and other provider services result in inurement or impermissible private benefit;
    iii. Whether partnership and joint venture arrangements and arrangements with management service organizations and physician hospital organizations conform to written policies, are properly recorded, reflect reasonable payments for goods and services, further WRHS's charitable purposes and do not result in inurement or impermissible private benefit;
    iv. Whether agreements to provide health care and agreements with other health care providers, employees, and third party payers further WRHS's charitable purposes and do not result in inurement or impermissible private benefit; and
    v. Whether relationships with Board members and management comply with the conflict of interest policy and other Board policies. At a minimum, management shall use the prior year's "Conflict of Interest Statements" as a basis to make the periodic review.
3. Annually and/or on an "as needed" basis, the Chairman of the Finance Committee will meet with management and any other individuals to discuss in detail all reportable conflicts of interest and to review in detail what steps, documentation, procedures, etc. have been put into place to document that each reportable conflict of interest has been handled in accordance with the Compliance Policy, Conflict of Interest Policy, as well as sound business judgment and practice.
4. Independent Audit Procedures:
    i. During its annual audit, the independent auditors shall mail a "Conflict of Interest" statement form to all officers, directors, managers, and members of a committee with Board delegated powers. The completed statement will be returned directly to the Audit Firm, with a copy provided by the Audit Firm to the Board of Directors. The Audit Firm will prepare a summary list of such reportable conflicts and audit the reportable conflicts as they deem necessary.

ii. The auditors will present a "Conflict of Interest" letter to the Board annually reporting their findings, problems, etc., as well as providing the Board with a current summary list of all reportable conflicts of interest.

Use of Outside Experts

In conducting these periodic reviews, the Corporation may use outside experts. If outside experts are used, their use shall not relieve the Board of Directors of its responsibility to see that periodic reviews are conducted.

C. Governance

The Board of Directors of WRHS is committed to furthering the charitable interests of WRHS and to safeguarding charitable assets. It is for these reasons that the Board of Directors has implemented the following Governance Policy:

1. It is the policy of the WRHS Board of Directors to comply with all applicable federal, state local laws and regulations, both civil and criminal, as well as those pertaining to the tax exempt status of WRHS. As used in this policy, the term "White River Health System" or WRHS includes each of its divisions, subsidiaries, and operating or business units.

2. The Board of Directors shall be active and engaged in the activities of WRHS. It shall be composed of persons who are informed and active in overseeing WRHS operations and finances. Accordingly, the Board of Directors shall review the WRHS's annual tax returns each year prior to filing with the IRS to ensure that financial resources are used to further the charitable purpose of WRHS. Such tax returns shall be made available for public inspection.

3. The members of the Board of Directors shall be diverse and selected based on the needs of WRHS to further its mission. The majority of the Board of Directors shall be independent and shall represent a broad public interest.

4. The members of the Board of Directors owe a duty of loyalty and a duty of care to WRHS and shall avoid conflicts of interest that are detrimental to WRHS. Any actual or potential conflict of interest shall be disclosed by Board members annually, and any member with a conflict of interest shall refrain from voting on any matter affecting such conflict.

5. The Board of Directors shall oversee and approve all major investments made by WRHS.

6. The Board of Directors shall oversee and enforce the WRHS policies regarding executive compensation, charity care, conflicts of interest, whistleblower, joint ventures, and document retention.

7. The Board of Directors shall meet as often as necessary to address the needs of WRHS and shall document the minutes of each board and committee meeting contemporaneously.

8. The Board of Directors shall periodically audit, either directly or through board committees, WRHS compliance with applicable laws, rules and regulations, and WRHS policies.

D. Joint Venture Policy

WRHS is a non-profit corporation organized exclusively for the charitable purpose of promoting the health of the community. In order to further this purpose, WRHS may from time to time enter into joint ventures with for-profit organizations.

WRHS shall only enter into joint ventures where its participation furthers the charitable purpose of WRHS, and

where the business arrangement allows WRHS to act exclusively in furtherance of Its exempt purpose and only incidentally for the benefit of for-profit partners. Accordingly, any such business arrangements shall be structured so that WRHS has the control necessary to maintain that the joint venture's operations further the charitable purpose of promoting the health of a broad cross-section of the community.

Subject to the review and approval by in house legal counsel, any joint venture arrangements entered into by WRHS shall provide the following:

1. WRHS shall receive an ownership interest in the joint venture proportionate to its contribution.

2. All returns of capital and distributions of earnings shall be proportional to the ownership/Interest.

3. A majority of the governing board of the joint venture shall be chosen by WRHS.

4. A majority of the governing body must approve major decisions, including, without limitation, the annual capital and operating budgets; distribution of earnings; selection of key executives; acquisition or disposition of health care facilities; contracts in excess of a specific dollar amount threshold; changes to the types of services offered; and renewal or termination of any management agreements.

5. The joint venture's governing documents shall require it to operate in a manner furthering charitable purposes.

6. The joint venture's governing documents provide that directors have a duty to operate in a manner furthering charitable purposes and this duty may override their duty to operate for the financial benefit of the for-profit members.

7. All management contracts shall be for a definite term of years and terminable for cause.

8. The terms, fees, and conditions of any management agreements shall be reasonable in comparison to management contracts of other organizations providing similar services at similarly situated health care entities.

E. Administrative Compliance with HIPAA Privacy Regulation

Appointment of a Privacy Officer

The Privacy Officer is responsible for the development and Implementation of the WRHS Privacy Policies. The Privacy Officer has also been designated as the contact person for receiving complaints concerning violations of the WRHS Privacy Policy and as the person from whom additional information may be obtained concerning any of the Issues discussed In the WRHS Notice of Privacy Practices.

Training

WRHS will provide training for all WRHS workforce on the policies and procedures about protected health information. Education programs will address the degrees of access to protected health information.

All employees shall be trained during orientation on the policies and procedures concerning protected health Information.

The type, amount, date and name of WRHS workforce who receive training on the policies and procedures concerning protected health Information will be documented.

Complaints

WRHS will address any complaints by an Individual that involves a potential violation of such individual's privacy rights.

Any complaint regarding the privacy of protected health information is to be made in writing to:

White River Health System
Attention: Privacy Officer
P.O. Box 2197
Batesville, AR 72503
(870)262-3266

Upon receiving the complaint, the Privacy Officer will:

1. Document the complaint in the Complaint Log.
2. Document the date, time and name of person making the complaint in the Complaint Log.
3. Investigate the complaint.
4. Document the resolution of the complaint in the Complaint Log.
5. Communicate the outcome of the complaint with the individual filing the complaint.
6. The Privacy Officer is to communicate the number of complaints and resolutions during routine executive level meetings of WRHS.

Sanctions

WRHS employees who fail to comply with the policies and procedures regarding protected health information will be sanctioned.

If any WRHS employee fails to comply with any policy or procedure regarding protected health information, the WRHS policy on disciplinary action will be implemented.

The severity of discipline will be determined according to:

1. The severity of the violation.
2. If the violation was intentional or unintentional.
3. If the violation indicates a pattern or practice of improper use or release of protected health information.

The degree of discipline may range from a verbal warning to termination.

Each episode of WRHS employee discipline regarding protected health information is to be documented and reported to the Privacy Officer.

Documentation is to include:

1. Name of WRHS employee
2. Degree of violation
3. Location of violation
4. Date and time of violation
5. Disciplinary action provided

Mitigation

WRHS will, to the extent reasonably practical, mitigate any harmful effects from the inappropriate use or disclosure of protected health information.

When WRHS is notified that protected health information has been inappropriately used or disclosed, such facts will be communicated to the Privacy Officer.

If the protected health information has been inappropriately used or disclosed by any WRHS employee, appropriate sanctions will be implemented in accordance with WRHS policies.

If the protected health information has been inappropriately used or disclosed by a business associate, WRHS will:

1. Investigate the incident;
2. Counsel the business associate on the incident;
3. Monitor the business associate's performance for a reasonable period of time following the incident; and
4. If the business associate does not remedy the situation leading to the inappropriate use or disclosure, WRHS will consider actions up to termination of the business associate agreement.

Non-intimidation or Retaliatory Acts

WRHS will not intimidate, threaten, coerce, discriminate against or take any retaliatory action against any individual: (1) exercising any right provided for in the HIPAA Privacy Regulations; (2) for filing a complaint alleging that his privacy rights have been violated; (3) assisting, testifying or participating in any compliance review or other proceeding concerning an alleged violation of the HIPAA Privacy Regulations; or (4) opposing any act not allowed under the HIPAA Privacy Regulations.

No Waiver of Rights

WRHS will not require any individual to waive any rights provided under the HIPAA Privacy Regulations as a condition of providing treatment or services to the Individual.

Documentation

WRHS will retain documentation of its HIPAA Privacy Policies in written or electronic form for a period of six (6) years from the later of the date such policies were created or the date when such policies were last in effect.

WRHS will also retain documentation of its compliance with all administrative requirements of the HIPAA Privacy Regulations for a period of six (6) years.

F. Transfer of Patient with Unstable Medical Condition or Active Labor

Examination of Emergency Room patients and women in active labor - All persons who present to WRHS's Emergency Departments requesting examination or treatment will receive a medical screening examination within the capabilities of the hospital to determine if an emergency medical condition exists.

1. If the Emergency Department physician is not immediately available, a Registered Nurse shall preliminarily triage the patient and will completely and adequately document the assessment.
2. Either the Emergency Department contract physician or the patient's private physician, according to the patient's expressed preference will examine the patient in a timely manner.
3. The physician shall assess the patient. This assessment will be fully and adequately documented.
    i. If another WRHS physician subsequently is requested to care for the patient on consultation or at the patient's request, the original physician remains responsible for the patient until the other physician arrives and takes charge of the patient's care.
4. Treatment of Obstetric Patients
    i. The ED Physician per ED policy will screen OB patients with an illness not related to the pregnancy.
    ii. If labor contractions, or pregnancy complications exist per the nursing triage assessment or ED medical screening exam, the patient will be referred to the OB on-call Physician for an OB medical screening exam.
    iii. If either physician determines that transfer is a necessity, the patient's condition will be stabilized prior to transfer.

Transfer of patients who have not been stabilized or who are in active labor will meet the following conditions.

1. No patient who has not received stabilization measures or is in active labor may be transferred:
    i. Unless the individual or his/her legal representative requests the transfer and signs "Request for Transfer" or,
    ii. The physician states clearly in the medical record that the risks caused by the transfer *are* less than the benefits to be received by treatment at another hospital. The specific risks and benefits will be referenced in the statement.
2. If the individual is deemed by the physician to require medical care and/or transfer and the patient refuses, all reasonable measures will be taken to have the patient or responsible party sign a "Refusal of Recommended Treatment or Transfer."
3. The patient may be transferred only when:
    i. It is determined that the receiving facility has adequate capacity and capability to treat the patient.
    ii. The receiving facility has agreed to accept the patient's care and provide appropriate treatment. The Nurse Manager, House Charge, Charge Nurse or designee will call the unit to receive the patient and verify admission.
    iii. The physician has written an order authorizing the transfer. This may be a verbal order.
4. Appropriate medical records will be sent with the patient. If the patient is transferred from a medical/surgical unit, the H & P, Discharge Summary, Pathology and Operative Reports, as well as other pertinent reports are copied and sent with the patient in addition to the Transfer Record. If transferred from the Emergency Department, copies of the Emergency Room Record, and copies of all pertinent diagnostic studies will be sent also.

Documentation of the transfer process will include the following:

1. Documentation of the stabilization and/or intervention to achieve optimum status possible.
    i. The measures taken and treatment implemented
    ii. A description of the patient's response to treatment
    iii. Measures taken to prevent (further) deterioration.
2. Consent of the receiving facility to accept the patient will be documented in the medical record and will include:
    i. The receiving facility
    ii. The name of the physician who has consented to accept care of the patient
    iii. The date and time of acceptance.
3. The medical record will include documentation of:
    i. The information given to the receiving facility
    ii. The suspected diagnosis
    iii. The patient's stabilized condition
    iv. Any staff member or physician at White River Medical Center who gives information to the receiving facility
    v. A record of information transmitted and/or sent with the patient
    vi. The information describing responsibility for the patient during transfer and transport to the receiving facility.
4. The physician's order to transfer the patient to another hospital will include:
    i. The destination *(name of facility)*
    ii. The name of the physician who will assume medical care and responsibility for the patient
    iii. A certification by the physician that the benefits of transfer outweigh the risks
    iv. The type of transportation required
    v. The specific category of professional personnel required to accompany the patient
    vi. Any equipment, supplies, or medications that may be required in transit with orders governing their use.

5. If the patient or a responsible party requests transfer, that fact will be recorded in the patient's medical record and will include:
    i. Explanation of the risks for transfer to the patient
    ii. An indication of the informed consent to the transfer
    iii. A description of the status or authority of any patient representative.
6. Certificate of Transfer will be completed and signed by the patient or responsible party, Shift Supervisor, or designee and physician prior to the transfer. All reasonable measures will be taken to obtain the patient's or responsible party's informed consent and signature. The Certificate of Transfer will be a part of the patient's permanent medical record. The first carbon will be sent with the patient. The second carbon will be sent to the director of the department from which the patient is transferred and then forwarded to the Nursing Office. The director will report quality assurance data. These copies will also be kept for no less than five (5) years.

With each transfer of a patient to another health care facility, the nurse caring for the patient will notify the Shift Supervisor/Nurse Manager or designee for the patient. They will affirm that each step of the above procedure has occurred and will verify the completion of the Certificate of Transfer. In the event that one or more criteria are not met, they will notify the physician of the proper steps which need to occur. The Administrator-On-Call will be consulted as deemed necessary by the Shift Supervisor or physician. A designee may complete the actual paper work, however the Nurse Manager or Shift Supervisor must be notified of the transfer and review transfer sheets to assure accuracy prior to transfer. Refer the checklist to the Administrative Assistant for Nursing. These will be kept on file for no less than five (5) years.

When transferring a psychiatric patient to the Arkansas State Hospital, all criteria herein apply. It is also essential that a consultation by the local Arkansas State Hospital affiliate be obtained.

- Call 1-800-592-9503, and explain circumstances of transfer and which physician at State Health has accepted care of the patient. A caseworker from North Arkansas Human Services Center will be dispatched to screen and authorize the transfer.

In Accordance with the Center for Medicare and Medicaid Services (CMS) guidelines, the 250 yard designation for WRHS to respond to emergencies is as follows:
1. Main Building- Main WRHS Hospital Building Complex
2. 250 Yard Boundary -
    i. Beginning curb of Sidney Street- West Boundary
    ii. Beginning curb of Harrison Street- North Boundary
    iii. Beginning curb of Hospital Circle Street- East
    iv. Boundary Beginning curb of Virginia Drive- South Boundary
3. In the event an individual requires medical assistance within the above boundary, they will be offered a medical screening exam within the capabilities of the Emergency Department. If the individual refuses examination or care, then a Release of Responsibility Form should be completed and turned into the Risk Management Department.

We expect all employees of WRHS to act responsibly in providing medical care within or outside the boundaries of the 250 yard rule.

G. EMTALA Violation

Transfers out of any White River Health System facility should fall into one of the following categories:
1. Patient request for transfer or
2. Level of care required is not provided by the facility.

If the patient requires services the WRHS institution cannot provide, such as pediatric inpatient psychiatric care

or acute alcohol or drug detoxification, patient transfer is required for patient safety and reasons for the transfer should be documented in the patient record.

The decision to transfer a patient to a receiving facility is always made based on patient need for services. Clinically pertinent data should be provided to the receiving institution and determination of the need for inpatient treatment documented in the record.

Any time a receiving facility refuses a patient transfer based on payment methodology, House Charge should be notified.

House Charge should contact the proposed receiving facility to discuss the reasons for refusal. If, after discussion, House Charge believes the decision to refuse transfer is based on the patient's ability to pay, the Administrator-On-Call will be notified.

The Administrator-On-Call will review the case and its documentation and contact the administrator on call at the receiving facility to discuss the transfer.

If this does not bring resolution to the situation, alternative arrangements for the patient's care should be made and implemented.

The next working day the CEO/Administrator will be notified of the situation and will review the case. If it is felt that the refusal to accept transfer violates EMTALA regulations, the CEO will contact the receiving facility’s CEO and discuss the case. Further action will be dependent on the EMTALA guidelines.

Code of Conduct

White River Health System

Board Adopted: August 22, 1997

Revised: _____

Code of Conduct Table of Contents

I. General Statement

White River Health System ("WRHS") is committed to integrity as the fundamental guiding principle for its employees and others who act on its behalf, and has prepared this Code of Conduct to reaffirm this commitment. The guidelines contained in this Code are designed to assist you in making the right choices when confronted with difficult situations. This Code imposes requirements that are often more exacting than those mandated by law, reflecting our goal of conducting ourselves with the highest level of integrity. The willingness of each of us to raise ethical and legal concerns is essential. Ultimately, the responsibility for ethical behavior rests with each of us in the exercise of our independent judgment.

WRHS also expects each employee to recognize and avoid activities and relationships that involve or might appear to involve conflicts of interest, and behavior that may cause embarrassment to WRHS or compromise its integrity. The following principles are intended to guide employees in recognizing these situations:

- WRHS and its employees will abide by the letter and spirit of all applicable laws and regulations and will act in such a manner that the full disclosure of all facts related to any activity will reflect favorably upon the Health System.

- WRHS and its employees will adhere to the highest ethical standards of conduct in all business activities and will act in a manner that enhances the Health System's standing as a vigorous and ethical contributor within the community.

- WRHS will deal fairly and honestly with those who are affected by our actions and treat them as we would expect them to treat us if the situation were reversed.

- WRHS will undertake only those activities that will withstand public scrutiny and not pursue any course of action which involves a violation of the law or these principles.

- WRHS will promote relationships based on mutual trust and respect and provide an environment in which individuals may question a practice without fear of adverse consequences.

- Each of us will abide by WRHS's Conflict of Interest Policy and will disclose any potential conflict of interest we may have regarding our responsibilities to the Health System and will remove the conflict as required.

We expect outside colleagues, e.g., vendors, consultants and others whose actions could be contributed to the Health System, to adhere to the same standards in their dealings with us and with others on our behalf.

An employee who has a question regarding the application or interpretation of the Code should use the procedure specified in Section IX, Compliance with the Code.

II. Conducting WRHS’s Business

WRHS's activities involve thousands of transactions each day. Obviously, we must have strict rules to guard against fraud of dishonesty and guidelines for addressing possible problems that may arise.

If you detect or suspect any behavior which you believe is or may be improper or inconsistent with the guidelines contained in this Code or the law on the part of any employee or agent of WRHS or any person with whom WRHS deals, you should report it immediately so that the appropriate investigation is initiated. (See

Section IX, Compliance with the Code).

Referral by WRHS for prosecution will be made when appropriate after review by in house legal counsel.

Compliance with Anti-Kickback and Self-Referral Laws

Federal law specifically prohibits any form of kickback, bribe, or rebate made directly or indirectly, overtly, or covertly, in cash or in kind to induce the purchase, recommendation to purchase, or referral of any kind of health care goods, services, or items paid by Medicare or Medicaid program. The term "kickback" means the giving of remuneration, which is interpreted under the law as anything of value. Under the federal law, the offense is classified as a felony and is punishable by fines and imprisonment for up to five years.

Federal and state "anti-referral" laws impose substantial penalties relative to billing for services referred by physicians or other health care practitioners who have a contractual or business relationship with the Health System. You should become familiar with these laws and assure that all of your activities are conducted in such a manner that no question may arise as to whether any of these laws have been violated.

Any question concerning these laws or any business arrangement subject to anti-kickback or anti-referral laws should be directed to the Compliance Officer (“CO”).

To list everything that may constitute an improper inducement under the anti-kickback laws would not be possible, but one thing is clear: WRHS must scrupulously avoid being either the one who offers or the recipient of an improper inducement. Care must be taken in structuring relationships with persons not employed by WRHS so as not to create a situation where WRHS appears to be offering an improper inducement to those who may be in a position to refer or influence the referral of patients to WRHS. For example, the offering of free goods or services, or those priced below market value, to physicians for the purpose of influencing them to refer patients to, or utilize the professional services offered by WRHS would be improper.

As a provider of patient care, WRHS also should not receive any improper inducement from its vendors to influence it in making decisions regarding the use of particular products or the referral or recommendations of patients to other providers of goods and services paid for by Medicare and Medicaid. For example, free, or at below- market value, goods or services from vendors, awards, discounts, prizes or other forms of remuneration may be treated as a "kickback" even if given as part of a promotional program of a vendor or provider, e.g., pharmaceutical company, medical equipment supplier, etc. There are certain exceptions to these rules which permit discounts, rebates and allowances under appropriate circumstances, provided there is proper disclosure of the discount or other remuneration to third-party payers.

Before entering into any business or contractual relationship with any person or organization which may raise a question under the anti-kickback laws, or with any physician or other health care practitioner who makes or may make referrals to WRHS, please consult with the CO.

Likewise, it is a violation of WRHS's policy, and an offense for which dismissal will be considered, for any officer, employee or any other person acting on behalf of or in the name of WRHS to make or authorize the paying of any bribe, any payment for an illegal act, or any other use of WRHS resources which, although arguably not illegal, could be interpreted as improper or unwanted.

In general, any money, property or favor offered or given to induce someone to forego normal business or professional considerations in making decisions that affect WRHS constitutes improper use of a resource. Equally improper is any payment of any kind to consultants, agents, brokers, attorneys, other individuals, or firms if there is reason to suspect that some or all of the payment is to be used to do anything that is prohibited by this Code.

A useful test to apply in determining whether a payment-or any other transaction-is proper is whether such transaction, if disclosed publicly, could adversely affect the reputation of WRHS. Another useful principle to

follow is not to give anything to a vendor, client, or other person doing business with WRHS which you could not yourself accept under WRHS's policies (See Gifts and Entertainment) if it were offered to you under similar circumstances. If you have any doubts as to whether a payment is lawful, you should consult your supervisor or the CO.

Billing for WRHS

WRHS and its staff provide a wide range of services to patients and the community. Because of our mission, some of these services are provided at no charge or at reduced rates. In most cases, however, billing statements are provided to the patient or a third party payer responsible for payment. It is imperative that these statements accurately reflect the services actually provided, who performed the service, and the precise charges for those services, as well as all other pertinent data relating to the patient. It is of course fundamental that no one acting on behalf of WRHS would intentionally falsify a claim. Such a conduct is a crime, is never in the interest of WRHS, and will result in severe sanctions. Negligently prepared bills cause significant administrative problems as well as tarnish WRHS's reputation for professionalism. Billing errors as well as billing improprieties of any kind may expose WRHS to civil or criminal liability. Medicare, Medicaid, and other payers may only be billed for medically necessary services that are properly documented. Under the Medicare and Medicaid programs, an erroneous bill could, in certain circumstances, be deemed to be a "false claim."

Accordingly, all WRHS employees and health care professionals who provide billing information and all employees who perform technical or clerical tasks in connection with preparing or submitting billing statements are required to become familiar with and abide by WRHS 's billing rules. Each employee must use his or her best efforts to prevent and, where appropriate, report errors, improprieties, or suspicious circumstances in billing that could violate applicable laws and regulations.

If you have knowledge of any billing errors or improprieties, or if you suspect an individual 's conduct with regard to billing is inconsistent with WRHS 's billing rules, this information must be reported to your supervisor or to the CO. Failure to report a suspected billing error or impropriety of any type may result in discipline up to, and including, dismissal.

Tax

WRHS is a charity, exempt from taxation by the federal, state, and local governments. In order to maintain this exemption, which is critical to WRHS 's survival, WRHS must operate for the benefit of the community and must avoid what the tax law calls "private inurement" and "private benefit." All nonexempt individuals or entities must pay fair market value for use of WRHS services or property. Violation of the tax law can give rise to criminal penalties as well. Questions on tax issues should be referred to the CO. Care must also be taken that WRHS's sales tax exemption is used only for legitimate WRHS activities. Personal items should not be purchased through WRHS even if WRHS is reimbursed by the employee.

All appropriate taxes must be withheld from the employees' wages, and the use of a purchase order to compensate individuals must be limited to true independent contractors and first cleared by the Chief Executive Officer or Chief Financial Officer.

WRHS has issued tax-exempt bonds, which are secured by revenues of WRHS. These bonds contain restrictions on the use of this property and on other WRHS activities which, if violated, could jeopardize WRHS 's ability to borrow money in the future. Questions on these issues should be referred to the Chief Financial Officer.

Emergency Care

WRHS is required by federal law to provide a medical screening examination, regardless of ability to pay, to patients who present to the Emergency Department and request examination. If the patient has an emergency medical condition, WRHS must treat and admit the patient, and can only transfer him or her after he or she has been stabilized. With respect to any person who is in need of emergency hospitalization, WRHS may not before admission question the patient or any member of his or her family concerning insurance, credit, or payment of charges, provided that the patient or a member of his or her family shall agree to supply such information

promptly after the patient's admission. All Emergency Department employees should be aware of WRHS's policy in this regard. Special restrictions govern the transfer process. Failure to comply with the detailed requirements of the federal law can subject WRHS or its staff to civil or criminal penalties. Questions should be referred to the Chief Executive Officer or Chief Medical Officer.

Pharmaceuticals, Prescription Drugs, Controlled Substances

Many of WRHS's employees have responsibility for, or access to, prescription drugs, controlled substances, hypodermic needles, drug samples, and other regulated pharmaceuticals. WRHS is legally responsible for the proper distribution and handling of these pharmaceutical products. Federal and state laws covering prescription drugs and controlled substances are intended to maintain the integrity of our national drug distribution system and protect consumers by assuring that prescription drugs are safe and properly labeled.

These laws include prohibition against diversion of any prescription drug or controlled substance, including a drug sample, in any amount for any reason to an unauthorized individual or entity. The distribution of adulterated, misbranded, mislabeled, expired or diverted pharmaceuticals is a violation of federal and state law for which severe criminal penalties may be imposed on individual violators as well as on WRHS.

It is WRHS's policy that all employees be both diligent and vigilant in carrying out their obligations to handle and dispense WRHS’s prescription drugs and controlled substances in accordance with all applicable laws, regulations, WRHS procedures. These WRHS procedures and policies are available in written form from Administration.

Every professional employee, whether physician, nurse, pharmacist, or any other licensed individual authorized to prescribe, dispense, or handle prescription drugs or controlled substances, is expected to maintain the highest professional standards in safeguarding pharmaceuticals of all kinds and in preventing unauthorized access to them. This includes adherence to laws and regulations governing procedures for securing scheduled controlled substances and for their return or destruction.

No prescription drug or controlled substance may be sold, transferred, or otherwise distributed unless authorized by a written WRHS policy or the appropriate WRHS individual charged with such responsibility. Nonprofit hospitals, including WRHS, are permitted by an exception to federal antitrust and price discrimination laws to purchase drugs at a specially discounted price. However, the drugs dispensed by WRHS's pharmacy are restricted to the WRHS employees, students, and staff physicians for their personal use or for the use of their dependents. Drugs dispensed by WRHS 's pharmacy may NOT, however be used by non-dependents or by staff physicians for their private practice without the express approval of the Chief Executive Officer.

Any violation of any law or any WRHS policy involving prescription drugs, controlled substances, or other pharmaceuticals will constitute grounds for dismissal. Each employee is expected to protect the integrity of WRHS by safeguarding the drugs entrusted to us for appropriate institutional medical use. If you become aware of any potential lapses in security, or any actual infringement of any law, policy or regulation relating to drugs, you must advise your supervisor or the CO immediately.

III. Research and Grant Requirements

The commitment of WRHS to integrity encompasses all research and grant proposals and activities, whether funded by government agencies, such as the National Institutes of Health, the United States Public Health Service, the Federal Food and Drug Administration, or by private sources. WRHS has established policies and procedures to insure that research projects and grants are conducted in a manner that is consistent with federal, state, local, and WRHS rules and regulations. It is expected that as members of the scientific community, staff will become familiar with these policies and procedures as well as the laws, rules and regulations governing research and grants.

Conflicts of Interest and Improper Referrals

It is extremely important to identify as early as possible in the grant-writing process any conflicts of interest between sources of grant funds and the WRHS recipient. Conflicts of interest would include any actual or potential financial interest of a grant recipient in the outcome of the research. Such conflicts are particularly likely to arise where grants are funded by private sources, which may include pharmaceutical companies and vendors of health care products or services. Researchers must abide by WRHS's Conflict of Interest Policy, a copy of which is available from Administration, and the American Medical Association ("AMA")'s guidelines on clinical investigation Code of Medical Ethics, Section 2.07 (1994 Edition). A copy of the AMA guidelines is available from WRHS. All conflicts must be reported to the CO.

Researchers must be vigilant in considering whether grants could involve improper inducements for the referral of patients to WRHS. This could occur, for example, in a study of drug efficacy underwritten by a pharmaceutical company if the protocol were not appropriately designed. If improper, such referral practices would constitute "kickbacks" in violation of federal law. Section II describes kickbacks and related issues in greater detail (see Section II, Compliance with Anti-Kickback and Self-Referral Laws). Any questions concerning whether the anti-kickback or other law may be involved in a research proposal should be directed to the CO. Care must be taken to be sure that the purpose of the research and the protocol are consistent with proper objectives, and that research is conducted so as to adhere to the approved protocol.

Scientific Misconduct

"Scientific misconduct" means fabrication, falsification, plagiarism, or other practices that seriously deviate from practices that are commonly accepted within the scientific community for proposing, conducting, or reporting research. It does not include honest errors or honest differences in interpretation or judgment of data.

WRHS defines "scientific misconduct" also to include failure to submit research projects for any approval that may be required, to obtain informed consent in accordance with WRHS's Informed Consent Policy, or to comply with the Conflict of Interest Policy or any other WRHS Policy regarding research activities. Fiscal improprieties and issues concerning the ethical treatment of human or animal subjects are also included in the WRHS's definition of scientific misconduct. In addition to the rise of serious federal and state penalties, scientific misconduct is a violation of WRHS's policy, and an offense for which dismissal will be considered.

Each person employed by or doing research under the auspices of WRHS must report to the CO any instance of scientific misconduct which he or she believes may have occurred or any allegations of scientific misconduct which are brought to his or her attention. WRHS has written guidelines setting out the process for dealing with alleged or apparent misconduct. The process is intended to protect the rights and reputation of all those who may be involved, and to ensure that the integrity of the Health System is maintained in all research activities.

Grants

All grant writing activity that is conducted on behalf of WRHS should be conducted in accordance with all laws, rules and regulations governing such grants and any specific guidelines imposed by the grantor. Once received, grant funds must be disbursed and accounted for pursuant to the grantor's requirements and in accordance with all laws, rules and regulations governing grants.

IV. Political Participation

Participation in the political process is one of every American's most basic rights. Federal and state laws, however, limit the nature and extent of organizational political participation.

Federal law and WRHS's policy also state that no one will be reimbursed for personal political contributions. Personal compensation will not be altered in any way under any circumstances to reflect such contributions.

WRHS encourages employees to participate in the American political process if they so desire. They may make personal political contribution or communicate their beliefs to elected officials.

It is important however, to distinguish between personal and organizational political activities. As a responsible corporate citizen, WRHS occasionally will speak out on issues of importance to it. Senior management is responsible for developing WRHS's position on relevant legislative and regulatory issues.

Unless you are specifically requested by WRHS to represent it before legislative or other governmental bodies, be sure you clearly label any personal communications with legislators as your own beliefs. If you are contacted by legislators or regulators regarding WRHS's position on public issues, you should refer them to Administration.

Lobbying

Certain management personnel may periodically be called upon by WRHS to make contact with members of city, county, state, or federal legislative bodies and other officials to set forth and advocate for WRHS's position on issues. These persons are expected to abide by all applicable laws at all times. Any person who attempts to influence any legislative, executive, or other governmental action, official, or employee on behalf of WRHS may be required to register as a lobbyist and file certain reports concerning his or her activities. There are also registration and reporting requirements as well as explicit limitations on lobbying that apply to WRHS. In addition, some laws provide rules of conduct for lobbyists. Federal law prohibits giving anything of value to any federal public official or person elected to be a public official in order to influence a decision by such official. In order to avoid any ambiguity in such matters, WRHS's policy is to prohibit the giving of gifts, meals or gratuities to federal officials without prior authorization, as discussed in Section V. Doing Business With the Government. To assure that these laws and policies are fully complied with, it is expected that no employee will engage in lobbying without prior authorization from Administration.

WRHS may also engage lobbyists or lobby firms to help promote its interests and has established internal controls to assure that all activities are legal. Written authorization must be obtained from the Chief Executive Officer prior to engaging any lobbyist, outside legal counsel, or consultant to lobby for or otherwise WRHS's interests on any legislative, regulatory, or other governmental issue. The following evidence must be submitted along with the proper request for authorization to justify the engagement.

- The purpose for the engagement and the nature and extent of services to be performed.
- The basis for selecting the proposed individual, firm, or company.
- The agreed-upon fee and the means by which the fee was determined to be reasonable and appropriate for the services to be performed.

All requests for reimbursement of expenses incurred by a lobbyist must be submitted within thirty (30) days after the expenses are incurred and must also be accompanied by a specific expense reporting form completed and signed by that lobbyist.

V. Doing Business with the Government

Medicare and Medicaid Requirements

WRHS participates in both the Medicare and Medicaid programs. Both programs are governed by complicated laws and regulations which impose strict requirements on providers that are significantly different from and more extensive than those one encounters in non-government commercial contracts. For example, Medicare and Medicaid have very complex payment guidelines that identify not only the circumstances under which, but also how much those programs will reimburse WRHS for goods and services rendered to patients covered under those programs. These guidelines are often different than directives received from other third party payers. Violation of Medicare and Medicaid laws and regulations can result in criminal sanctions being imposed not only on the persons actually involved but also on the organization on whose behalf those persons act. Moreover, if WRHS was found to be involved, it might be excluded from participating entirely in the Medicare and Medicaid programs. It is essential, therefore, that we strictly comply with all Medicare and Medicaid laws, rules and regulations.

Hiring of Former Government Employees

Very specific rules exist to eliminate even the appearance of a conflict of interest by former government employees who, upon termination of their government service, seek employment with those who do business with government. You should obtain clearance from the Chief Executive Officer prior to discussing the employment or possible retention as a consultant of any current or former government employee.

Both WRHS and any employee or consultant who was a former government employee must comply with all applicable rules while working on WRHS ‘s behalf.

No Gifts, Meals, or Gratuities for Government Personnel

You may not provide or pay for meals, refreshments, travel, or lodging expenses for government employees. Very strict guidelines prohibit any type of gratuity, with very few exceptions, and your strict compliance is required. Unlike in other circumstances, the laws regarding this issue could be violated if anything of value is given to a governmental employee even if there is no intent to influence an official action or decision. Therefore, no employee should entertain a public official without authorization from Administration.

VI. Employee Loyalty and Conflicts of Interest

WRHS expects its employees to serve WRHS with undivided loyalty. You should put WRHS's interests ahead of any other business and commercial interest you may have as an individual. (See also Section II, Conducting WRHS's Business). You should avoid situations in which a conflict of interest, or the appearance of a conflict, could arise. For more complete guidance as to WRHS's policy on these types of issues, please refer to the Conflict of Interest policy.

VII. Use of Health System Information

Safeguarding the Privacy of Our Patient

Our professions require that we gather a great deal of personal information about individuals. Therefore, we must carefully avoid any unwarranted invasion of individual’s right to privacy. This applies to information about our patients and our employees. For this reason, and to assure the accuracy of the information we retain, the following guidelines apply:

- To protect individuals against misuse of information identifiable to them, limit access to that information, except to the extent permitted by WRHS policy.

- Use only legitimate means to collect the information and, whenever practical, obtain it directly from the individual concerned.

- Special confidentiality rules apply to patients in drug and alcohol treatment programs, as well as disclosure of information regarding a patient's HIV status. When release of any information with respect to patients with these illnesses is contemplated, these rules must be adhered to carefully.

Any employee or agent of WRHS who engages in any unauthorized disclosure of information in violation of the privacy rights of our patients or others may be subject to immediate termination in addition to possible civil or criminal sanctions. Any person who becomes aware of such unauthorized disclosure should report it immediately.

Confidentiality of WRHS Information

One of WRHS's most valuable assets is its body of confidential information. The widespread use of computer terminals and computer systems have caused this information to be accessible to many employees. Failure to protect this information adequately can lead to the loss of confidential data that may place WRHS legally at risk. Because of this risk of harm to WRHS, its employees, and patients, no employee shall, without the written consent of WRHS, during the term of employment or thereafter, use for the benefit of such employee or others, or disclose to others any confidential information obtained during the course of employment.

Confidential information includes WRHS's methods, processes, techniques, computer software, equipment, service marks, copyrights, research data, clinical and pharmacological data, marketing and sales information, personnel data, patient lists, financial data, plans, and all other know-how and trade secrets which are in the possession of WRHS and which have not been published or disclosed to the general public.

As an employee, you are responsible and accountable for the integrity and protection of confidential information and must take steps to protect information that has been entrusted to you. For example, you must not make inappropriate modifications of information or destroy or disclose information except as authorized. Documents containing sensitive data, including information concerning patients, should be handled carefully during work hours and must be properly secured at the end of the business day. Particular attention must be paid to the security of data stored on the computer system. If you observe individuals that you do not recognize using terminal in your area, immediately report this to your supervisor.

Information Owned by Others

Like WRHS, other organizations have intellectual property they want to protect. So do individuals. Also like the Health System, these other parties are sometimes willing to disclose their confidential information for a particular purpose. If you are on the receiving end of another party's confidential information, you must proceed with caution to prevent any accusations that you or WRHS misappropriated or misused the information.

To avoid the risk of you or WRHS being accused of misappropriating or misusing someone's confidential or restricted information, there are certain steps you should take before receiving such information. The receipt of confidential or restricted information whether oral, visual, or written must not take place until the terms of its use have been formally agreed to by WRHS and the other party. That means a written agreement approved by Administration. Furthermore, unless otherwise delegated, establishing such an agreement for the receipt of confidential or restricted information of another party will require the prior written approval of an appropriate WRHS Administrator. Once another party's confidential or restricted information is properly in your hands, you must not use, copy, distribute, or disclose that information unless you do so in accordance with the terms of the agreement.

Special care should be taken in acquiring software from others as intellectual property software is protected by copyright laws and may also be protected by patent, trade secret laws, or as confidential information. Such software includes computer programs, databases, and related documentation owned by the party with whom you are dealing or by another party. Before you accept software or sign a license agreement, you must follow

established WRHS procedures. The terms and conditions of such license agreements - such as provisions not to copy or distribute programs - must be strictly followed. Also, if you acquire software for your personally-owned equipment, you should not copy any part of such software in any work you do for WRHS, place such software on any WRHS-owned computer systems, or generally bring such software onto WRHS premises.

In any cases do not take the status of information for granted. If you have information in your possession that you believe may be confidential to a third party or may have restrictions placed on its use, you should consult with Administration.

Records Retention/Destruction

WRHS is required by law to maintain certain types of medical and business records, usually for a specified period of time. Failure to retain such documents for such minimum period could subject WRHS to penalties and fines, cause the loss of rights, obstruct justice, place WRHS in contempt of court, or put WRHS at a serious disadvantage in litigation. Accordingly, WRHS has established controls to assure retention for required periods and timely destruction of retrievable records, such as hard copies and records on computers, electronic systems, microfiche, and microfilm. Even if a document is retained for the minimum period, legal liability could still result if a document is destroyed before its schedule destruction date.

You are expected to comply fully with the records retention and destruction schedule for the department in which you work. If you believe that documents should be saved beyond the applicable retention period, consult your supervisor, who in turn should contact Administration.

It is likewise critical to the successful accomplishment of WRHS's professional goals that its records are accurately completed and maintained consistent with proper business practices. Many of WRHS's records serve as a basis for treatment decisions for its patients, as a compilation of goods and services rendered for billing purposes, and as a recordation of historical courses of treatment. Each of these functions serves as an indispensable role in enabling WRHS to fulfill its obligation to its patients, the medical and nursing staff, and the various payers for goods and services. Consequently, the proper and contemporaneous creation of fully accurate and complete records is a duty of each member of the WRHS.

Government Investigations

Given the increased vigilance by law enforcement agencies in the health care arena, it is important that WRHS establish definitive guidelines on how and when to respond to government inquiries. Inaccurate or incomplete information provided to government officials in response to their inquiries will more often than not generate complications for WRHS and possibly frustrate the legitimate purposes of the inquiry. Unauthorized disclosure of information may jeopardize our patients' rights to privacy and expose the organization to liability. Therefore, we must adhere to the following procedures to ensure WRHS responds in a proper manner to all government investigations.

Any employee of WRHS who is approached by any federal or state law enforcement agency seeking information about any aspect of the operations of WRHS or the job-related activities of any of WRHS's offices, employees, or agents should call Administration before turning over any information. Two agencies are entitled, by law, to immediate access to information: the Office of the Inspector General of the United States Department of Health and Human Services and Arkansas Medicaid Fraud Control Units. Proper identification must be presented by officials of either of these agencies before access can be provided. In almost all cases, when a request by personnel of either agency is made, access to the requested information should be delayed pending notification of Administration. Such notification should occur simultaneously with the requested access. Notification will ensure that the organization is aware of the inquiry, properly responds to it, and can take whatever action is necessary with regard to it. If access cannot be delayed pending notification of Administration, then Administration should be contacted simultaneously with allowing access to the data.

Other governmental agencies, however, may look at WRHS documents and other materials only with WRHS's consent or by proper legal process. These agencies include: The Federal Bureau of Investigation, the Drug Enforcement Administration, the United State Postal Inspector, the Arkansas Attorney General (with the

exception of the Medicaid Fraud Control Unit), the Independence County prosecutor, and local police departments.

To assure that government agencies are provided with the information to which they are entitled on a timely basis and, at the same time, to prevent the improper disclosure of private information, it is imperative that you contact Administration as promptly as possible after receipt of, or compliance with, any request for information that you receive. In addition, please be certain to (1) obtain the name and organization affiliation of all persons from whom a request for access to information is received or to whom access if permitted before any access is allowed, (2) maintain a written record of each and every document to which access is given, (3) keep a detailed record of all telephone contacts made, including specifically the name and affiliation of the parties to each conversation, the information requested and the response given during the conversation.

Specific confidentiality laws relating to medical records pertaining to AIDS and substance abuse (controlled drugs and alcohol) and to psychiatric records may limit the general authority of government investigators. Employees should be certain that any disclosure of such records complies with the policies and procedures of WRHS.

VIII. Human Resources

Commitment to Fairness

WRHS recognizes that its greatest strength lies in the talents and abilities of employees. To promote positive employee relations and to ensure an environment of fairness, WRHS has established the following commitments:

- To provide equal opportunity for employment and advancement on the basis of ability and aptitude without regard to race, color, creed, age, sex, or sexual orientation, disability, or national origin except where such is a bono fide occupational qualification.
- To protect the health and safety of employees in their work environment.
- To compensate employees according to their performance, and to provide equitable benefits within the framework of prevailing practices.

WRHS is committed to ensuring a work environment in which all individuals are treated with dignity and respect. Each employee has the right to work in a professional environment that promotes equal opportunity and is free of discriminatory practices. Discrimination or harassment, whether based on race, color, religion, sex, or sexual orientation, national origin, age, or disability is unacceptable and will not be tolerated. WRHS's Human Resources Department has developed a variety of policies in support of these commitments. Familiarity and adherence to these policies IS the responsibility of each employee.

IX. Compliance with the Code of Conduct

Questions Regarding the Code

The CO is responsible for implementation of WRHS's Compliance Plan, including the Code. The CO will work with others in WRHS, including the Compliance Coordinators, with respect to elements of implementation and enforcement of this Code of Conduct. An employee who has a question regarding the applicability or interpretation of the Code should direct the question to the CO in person, in writing, or by calling the CO. Correspondence relating to the Code should be addressed to the CO and marked "CONFIDENTIAL."

Reporting of Violations

As part of its commitment to ethical and legal conduct, WRHS expects its employees to bring to the attention of the CO, or any appropriate person designated by the CO, information regarding suspected improper conduct. The employee must immediately report such information to his or her supervisor or the CO. Employees are

required to come forward with any such information, without regard to the identity or position of the suspected offender. Reports to the CO may be made by calling the CO or writing to the CO concerning questions regarding the Code. Because failure to report criminal conduct can itself be understood to condone the crime, we emphasize the importance of reporting. Failure to report knowledge of wrongdoing may itself result in disciplinary action against those who fail to report. Any manager or officer receiving a report of a potential Code violation must likewise immediately advise the CO of such violation or possible violation. There will be no reprisals for good faith reporting of actual or possible violations of the Code. Where possible, the identity of the employees making the report will be kept confidential.

Investigation of Violations
All reported violations of the Code will be promptly investigated by WRHS and will be treated confidentially to the extent consistent with the WRHS's interests and its legal obligations.

All investigations by WRHS of wrongdoing will be directed by the CO. Employees are required to cooperate in the investigation of an alleged violation of the Code. If the result of the investigation indicates that corrective action is required, WRHS will decide what steps it should take to rectify the problem and avoid the likelihood of its recurrence.

Any material violation of criminal, civil, or administrative law as determined after investigation will be reported to the appropriate government agency after consultation with in house legal counsel. Such reporting will occur within a reasonable period of time after final determination that an offense has occurred.

Discipline for Violations
Disciplinary actions may be taken for:

- Authorization of or participation in actions that violate the Code.
- Failure to report a violation of the Code or to cooperate in an investigation.
- Failure by a violator's supervisors to detect and report a violation of the Code if such failure reflects inadequate supervision or lack of oversight.
- Retaliation against an individual for reporting a violation or possible violation of the Code.

Disciplinary action may, when appropriate, include dismissal. With respect to disciplinary action, principles of fairness will apply, including, when appropriate, review of a disciplinary decision.

Acknowledgement and Certification of Compliance
WRHS requires that employees at the ranks of Assistant Administrators and higher, Department heads, and all supervisors sign an acknowledgment confirming that they have received and read the Code of Conduct and understand it, and acknowledge that the Code has been communicated to all employees and agents under their supervision. In addition, each year these employees will be asked to submit an updated Annual Employee Attestation.

X. Individual Judgment

The foregoing guidelines are to help all of us better understand what we believe to be in the best interest of our employees, patients, those with whom we do business, and the public at large. Ultimately, however, you are left to depend on your own individual judgment in deciding on the correct course of action.

As you contemplate a particular situation, consideration of the following factors may help you arrive at a satisfactory answer:

- Is my action consistent with WRHS practices?
- Could my action give the appearance of impropriety?

- Will the action bring discredit to any employee or WRHS if disclosed fully to the public?
- Can I defend my action to my supervisor, other employees and to the general public?
- Does my action meet m y personal code of behavior?
- Does my action conform to the spirit of the Code?

Remember always to use good judgment and common sense. Whenever you see a situation where this purpose does not appear to be covered by the Code of Conduct, you have the responsibility to bring your concern to the attention of the CO.

APPENDIX B – Identity Theft

What is Identity Theft and How Could It Happen To Me?

Identity theft is a crime. Identity theft occurs when someone uses your personal information without your permission to commit fraud or other crimes, most commonly to obtain access to credit in your name. For example, an identity thief may steal your Social Security number and open, or attempt to open, a credit account under your name. Personal information includes:

- Social Security number
- Driver's License number
- Bank account number
- Credit card number
- Personal Identification Numbers (PINs)
- Mother's maiden name, or other information used as a security screen
- Passwords
- Any other piece of key information that can be used to gain access to a person's financial resources, or to assume a person's identity

How Does Identity Theft Occur?

An identity thief can steal your information in a variety of ways. Below are a few examples of how identity thieves may obtain your personal information.

- *Mail* — Identity thieves steal mail directly from your mailbox. When sending mail, such as bill payments, you could be inadvertently advertising your personal information to potential identity thieves simply by placing the red flag up on your mailbox.
- *Trash* — Identity thieves can steal personal information from documents or other items that you discard. They have been known to sort through trash for discarded receipts, credit card statements, bank account statements, credit card applications, and anything else that could contain personal information.
- Wallet or purse — One of the most common ways identity thieves obtain personal information is by stealing your wallet or purse.
- *Home* — Identity thieves can burglarize your home and steal important documents they may find, such as credit card and bank account statements, check books, Social Security Cards, drivers' licenses and birth certificates.
- *Relatives and friends* — A survey commissioned by the Better Business Bureau found that you are just as likely to have your identity stolen by a relative, friend or acquaintance as you are to have it stolen online. Relatives and friends conveniently have access to your personal information and all too often they are the culprits behind identity theft.
- *Computers* — Consumers routinely use personal computers for financial transactions. Identity thieves can illegally gain access to computers for the purpose of stealing your personal information.
- *Businesses* — Identity thieves can bribe an employee at a business who has access to personal information. In some instances, the employee can steal information and commit identity theft. Also, "security breaches" can occur by illegally accessing information found on computers. Breaches also may come from theft from the business, or from someone posing as a legitimate business client. Other breaches occur accidentally when no one intends to steal information.
- *E-mail or phone, "phishing," "pretexting"* — Identity thieves can send e-mails, posing as legitimate companies, requesting verification of your personal information. This is known as "phishing." Legitimate businesses will never request personal information from you by e-mail. Also, identity thieves may call you, posing as a legitimate company, requesting you verify your personal information, or they may contact an information source, posing as you, seeking personal information. This is known as "pretexting."

How Can I Protect Myself from Identify Theft?

Although there is no way to make sure that your personal information is totally safe, you can take steps to avoid becoming a victim.

Minimize Your Risks

- Protect your mail. Send and receive mail safely. Mail your bills from a secure location and don't leave sensitive mail sitting in your mailbox for extended periods.
- Shred documents with personal information. Shred or otherwise destroy any statements, documents, or records, which contain personal or financial information after they are no longer needed.
- Keep a close eye on personal documents and credit cards. Although there are always new schemes hatched to steal your identity, the most common form of identity theft continues to be obtaining personal information through lost or stolen documents, checkbooks or credit cards. Do not keep information that you don't need in your purse or wallet. Specifically, do not carry your Social Security Card with you unless you know you will need it that day. Do not keep personal identification numbers attached to credit, debit or ATM cards.
- Be careful about where you store your information at home. Store important information in a safe place in your home. Do not leave financial records lying around your house for prying eyes to see.
- Be safe online. Use anti-virus and anti-spyware software, as well as a firewall, and update them all regularly. Be sure to set up your operating system and web browser software properly, and update them regularly. Avoid using obvious passwords like your birth date, your mother's maiden name, or the last four digits of your Social Security number. For tips from the federal government and the technology industry about protecting yourself from Internet fraud, and securing your computer, please visit www.onguardonline.gov.
- Don't share personal information over the Internet. Never respond to an e-mail that asks you to transmit personal information over the Internet. Don't get reeled in by a "phishing" scam. Legitimate companies will not make such requests. Remember that your bank or credit card issuers already have your account numbers, PINs, access codes, passwords, Social Security number and other information they need. They won't e-mail you to ask for it.
- Beware of giving personal information over the phone. Know who you are dealing with, and don't fall for the "pretexting" con. When in doubt, hang up and get the business's phone number from an independent source.

How Can I Tell If My Identity Has Been Stolen?

Everyday due diligence is the best way for you to detect suspicious activity that may be the result of an identity theft.

- Review bank statements and credit card statements. Monitor your financial account statements for any unusual activity. Promptly report any unauthorized charges to the account provider.
- Check your credit report at least once a year. Everyone is allowed one free credit report per year from each of the three national credit bureaus: Equifax, Experian, and TransUnion. By checking your credit report you can determine whether accounts have been opened in your name without your knowledge. Also, you can check the accuracy of the report. You have the right to have inaccurate or outdated entries removed from your credit report. To learn how to obtain your free credit report, please visit www.annualcreditreport.com.

Red Flags

- Receiving unexpected bills or collection calls. Getting an account statement for an account that you did not authorize is an indication that you may be the victim of identity theft. Likewise, getting collection calls from a creditor or debt collector regarding an account that you did not authorize is an indication that you may be the victim of identity theft.
- Not receiving expected bills or account statements. If your monthly credit card statement stops coming to your address, this could be an indication that someone has stolen your mail or changed your account statement mailing address. Promptly report this to the account provider.
- Having a credit application denied when you have no reason to believe you have a problem with your credit history. Be sure to periodically review your credit report, and always review it again before you make an application for credit on a big purchase.

I'm a Victim, What Should I Do?

If you believe you are a victim of identity theft, we urge you to take the following steps as soon as possible:

1. File a Fraud Alert with one of the three national credit bureaus. The credit bureau with which you choose to file a fraud alert is required to contact the other two, which will then place a fraud alert on your credit reports with their bureau as well. Once a fraud alert has been placed on your credit file, if an application for credit is filed in your name, and the prospective creditor checks your credit report, the prospective creditor will be alerted to the

possibility of identity theft. That prospective creditor can then check directly with you before completing the credit transaction. Visit our resources page to obtain contact information for the three bureaus.

2. File an identity theft report with your local law enforcement agency.
3. Close any accounts that have been tampered with or opened fraudulently. It is imperative that you contact the company involved to dispute the fraudulent transactions or accounts. You should follow up with the company in writing. It is recommended that you send all correspondence by certified mail. Ask the company whether a fraud affidavit is required. If a fraud affidavit is required, the company may send you its specific affidavit or you can get an I.D. Theft affidavit from the publication Take Charge: Fighting Back Against Identity Theft. These materials are available at the Federal Trade Commission's national identity theft resource webpage.
4. File an Identity Theft complaint with the Federal Trade Commission online or call (877) IDTHEFT (438-4338).
5. Consider placing a Security Freeze on your credit report. Any person, whether victim of identity theft or not, may place a security freeze on their credit report. If you have been a victim of identity theft, or if you are 65or older, you may freeze your credit report without charge. A security freeze is designed to restrict access to your credit report and help prevent additional instances of identity theft.
6. Consider requesting an Identity Theft Passport provided by the Attorney General's Office. An application for the Identity Theft Passport is available here.

Fraud Alerts

A fraud alert is a statement that is placed on a credit bureau report that is intended to help consumers who have been a victim, or may have been a victim, of identity theft. A fraud alert is designed to stop an identity thief from using your personal information to open fraudulent credit accounts in your name. When a creditor or business reviews a credit report in which a fraud alert has been placed, they are prompted to verify the identity of the applicant using the information listed on the report. This may result in the creditor or business calling you directly or sending a letter or inquiry prior to granting the credit application. For this reason it is important to make sure your contact information is current on your credit report.

To place or rescind a credit bureau fraud alert, you need to contact only one of the three nationwide credit bureaus. By law, the credit bureaus are required to share fraud alert requests with the other bureaus. You will be required to provide appropriate proof of your identity, which may include your Social Security number, name, address, and other personal information the credit reporting company requests.

There are two types of credit bureau fraud alerts—an "initial alert" and an "extended alert."

- Initial Fraud Alert: An initial fraud alert is appropriate if your wallet has been stolen or if you suspect or believe your identity has been or will be compromised. By requesting an initial fraud alert you are entitled to one free credit report from each of the three nationwide credit bureaus. The initial fraud alert will last 90 days. It may be placed by calling one of the three nationwide credit bureaus.
- Extended Fraud Alert: An extended fraud alert is for a consumer who knows that he or she is a victim of identity theft. To place an extended fraud alert, you will be required to provide the credit bureau with a copy of an identity theft report, such as a police report, and appropriate proof of your identity as mentioned above. The extended fraud alert lasts seven years. By requesting an extended fraud alert, you're entitled to two free credit reports within 12 months from each of the three nationwide credit bureaus. Additionally, with the extended fraud alert, the consumer reporting companies will remove your name from marketing lists for prescreened credit offers for five years unless you ask them to put your name back on the list before then.

Here is the contact information for the three national credit bureaus:

- TransUnion: (800) -680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790
- Equifax: (800) 525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374- 0241
- Experian: (888) 397-3742; www.experian.com; P.O. Box 9554, Allen, TX 75013

Security Freeze

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. You should be aware,

however, that using a security freeze may delay or prevent the prompt approval of any subsequent request or application you make regarding a new loan, credit, mortgage, government services or payments, rental housing, employment, investment, license, cellular phone, utilities, digital signature, Internet credit card transaction, or other services, including an extension of credit at the point of sale.

When you place a security freeze on your credit report, you will be provided a personal identification number or password to use if you choose to remove the security freeze on your credit report or authorize the release of your credit report for a period of time after the security freeze is in place. To provide that authorization you must contact the national credit bureau and provide the following:

1. Your personal identification number or password.
2. Proper identification to verify your identity.
3. The proper information regarding the period of time for which the credit report shall be available.

The national credit bureau must authorize the release of your credit report for a period of time within 15 minutes or as soon as practical if good cause exists for the delay, and must remove a security freeze no later than three business days after receiving all of the above items by any method that the consumer reporting agency allows.

A security freeze does not stop all access to your credit report. Companies with which you have an existing account, or collection agencies acting on behalf of such companies, may still request information from your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

You have the right to bring a civil action against anyone, including a national credit bureau that willfully or negligently fails to comply with any requirement of the Arkansas Consumer Report Security Freeze Act.

A national credit bureau has the right to charge you up to $5 to place a security freeze on your credit report, to temporarily lift a security freeze on your credit report, or to remove a security freeze from your credit report. However, you shall not be charged any fee if you are 65 or older or if you are a victim of identity theft and have submitted, in conjunction with the security freeze request, a copy of a valid investigative report or incident report.

How To Request a Security Freeze

A consumer may request that a security freeze be placed on his or her consumer report by doing one of the following:

1. Sending his or her request in writing by mail to a national credit bureau.
2. Telephoning his or her request to a national credit bureau and providing over the telephone proper identification or personal identification information required by the national credit bureau.
3. Electronically forwarding his or her request to a national credit bureau through a secure electronic connection or a secure electronic mail connection if the connection is made available by the national credit bureau.

For detailed instructions on requesting a security freeze please contact the credit reporting agencies directly. Their contact information is as follows:

- Equifax: P.O. Box 740241, Atlanta, GA 30374; (800) 525-6285; www.equifax.com
- Experian: P.O. Box 9532, Allen, TX 75013; (888) 397-3742; www.experian.com
- TransUnion Fraud Victim Assistance Division: P.O. Box 6790, Fullerton, CA 92834-6790; (800) 680-7289; www.transunion.com

Identity Theft Passport Victim ID Card

In 2005, the Arkansas Legislature approved Act 744 “An Act to Provide for the Issuance of an Identity Theft Passport by the Attorney General to Victims of Financial Identity Theft.” In short, Act 744 gives the Attorney General authority to issue an Identity Theft Passport to an Arkansas resident who learns or reasonably suspects that he or she is a victim of financial identity fraud and who has filed a police report confirming that he or she is a victim of financial identity fraud. The Identity Theft Passport is a card, similar in appearance to a driver’s license, which is designed to assist financial identity fraud victims in reestablishing their good names. In addition, the Identity Theft Passport may help prevent a victim’s arrest for other criminal offenses committed by the identity thief.

- ID Theft Passport Victim Identification Card Application Instructions
- ID Theft Passport Victim Identification Card Application

Security or Data Breach

A Security Breach or Data Breach is one of the most common causes of disclosure of personal information. These breaches can expose the personal information of a few thousands, or even millions of individuals. It occurs when personal or otherwise sensitive information that is maintained by an entity is accessed in an unauthorized manner, or when that information is inadvertently exposed. Such an incident certainly increases one's risk of identity theft. However, it should be noted that not all personal information compromises result in identity theft.

The Arkansas Personal Information Protection Act requires entities that collect personal information use reasonable security procedures and practices to protect such information. Additionally, the law mandates that in the event such information is compromised, the entity must notify the affected individuals in a timely manner. Notification to individuals whose personal information has been compromised allows them to take steps to mitigate the potential misuse of their information.

Although it is not required by Arkansas law, many entities that experience a Security Breach will offer credit monitoring services at no charge to affected individuals, usually for a period of one year. Credit monitoring can be useful in this context; however, it is entirely up to you whether you want to take advantage of such an offer.

What Should I Do If I Receive a Security Breach Notification?

- If the compromised information relates to existing financial accounts, contact your financial institution to close or change the account information as soon as possible.
- Consider placing a Fraud Alert on your Credit Bureau Reports.
- Consider placing a Security Freeze on your Credit Bureau Reports.
- Periodically monitor your Credit Bureau Reports for any unusual activity and check for accuracy. Everyone is allowed one free credit report per year from each of the three major credit bureaus. To learn how to obtain your free annual credit report under Federal law, please visit www.annualcreditreport.com or call (877) 322-8228. A victim of fraud is eligible to receive one free credit report from each of the major credit bureaus. Requests for a free report based on a fraud claim should be made directly to the credit bureaus:
    - TransUnion: (800) 680-7289, www.transunion.com; P.O. Box 6790, Fullerton, CA 92834-6790
    - Experian: (888) 397-3742, www.experian.com;P.O. Box 9532, Allen, TX 75013
    - Equifax: (800) 525-6285, www.equifax.com;P.O. Box 740241, Atlanta, GA 30374-0241

Skimming

Skimming refers to the method by which information is stolen from an account-access device, such as a credit card, debit card, or ATM card. Typically card skimming occurs through the use of a handheld electronic swiping device; however, more sophisticated criminals have been able to manufacture skimming components that imitate legitimate card-reading devices like those found on ATMs and fuel pumps.

How do you avoid being a victim of skimming? Although you may not be able to prevent crime from happening, there are ways to protect yourself from this type of fraud.

- If at all possible, don't let your credit or debit card out of your sight.
- Take notice of your surroundings. If an ATM or fuel pump looks as if it's been tampered with, don't use it and notify the owner or management.
- Always review your account statements for any suspicious activity. If you detect an unauthorized charge, notify your financial institution as soon as possible. Timely reporting of an unauthorized charge will mitigate your liability.

References

My Identity. (n.d.). Retrieved 08 14, 2015, from www.gotyourbackarkansas.org:

http://www.gotyourbackarkansas.org/my-identity/

APPENDIX C – Annual Employee Attestation

To the best of my knowledge and belief, all practices and policies of White River Health System are legal and in compliance with state and federal regulations and laws.

Signature _____ Date _____

I do not agree with the above statement for the following specific reason(s):

_____

_____

_____

_____

_____

Signature _____ Date _____

I have been provided a copy of the Code of Conduct and Compliance Plan, I have read and understand these documents, and I agree to abide by all provisions of the Code of Conduct and the Compliance Plan. I have been informed that the Compliance Hotline numbers are (870) 612-3136 for local calls and 1-866-612-3136 for toll free calls. By agreeing to comply with the Code of Conduct, I acknowledge that I have a duty to report any suspected violations of the law or the standards of conduct to my immediate supervisor, Compliance Oversight Committee, or a Compliance Coordinator.

Signature _____ Date _____

APPENDIX D – Conflict of Interest Statement

Effective _____, _____

_____being a duly qualified and elected director of

_____ hereby state the following:

1. I have received and read a copy of the Corporation's Conflict of Interest Policy. I understand such policy and agree to abide by its terms and conditions.
2. I realize that my position as a director means that I have a fiduciary obligation toward the Corporation which requires that I act in the utmost good faith in all of my dealings in my capacity as a director. A part of this duty I owe as a director includes me not engaging in transactions which create a "conflict of interest."
3. I further understand that the Corporation is a charitable organization and in order to maintain its federal tax exemption, it must engage primarily in activities which accomplish one or more of its tax-exempt purposes.
4. A "conflict of Interest" is defined as a transaction with the Corporation in which a director of the Corporation has a direct or indirect financial Interest in the party with whom the Corporation Is conducting business. A director shall be considered to have a direct financial interest in a transaction any time the transaction could result in financial gain accruing to the director in his individual capacity. A director shall be considered to have an indirect financial interest in a transaction any time that the director has a material financial interest in the party dealing with the Corporation.
5. A Director has a "financial interest" if the director has, directly or indirectly, through business, investment or family
   i. an ownership or investment interest in any entity with which the Corporation has a transaction or arrangement, or
   ii. a compensation arrangement with the Corporation or with any entity or individual with which the Corporation has a transaction or arrangement, or
   iii. a potential ownership or investment interest in, or compensation arrangement with, any entity or individual with which the Corporation is negotiating a transaction or arrangement.

   (Compensation includes direct and indirect remuneration as well as gifts or favors that are substantial in nature.)
6. If I have any of the above mentioned arrangements listed in paragraph five (5), I will list them in Exhibit "A", which is attached hereto.
7. If my interests in the businesses or organizations listed in Exhibit "A" change within the following year, or if I acquire additional interests in businesses or organizations which may reasonably be expected to have a relationship or transaction with the Corporation that could create a conflict of interest, I will provide the board of directors with a written statement detailing any such change.
8. If any matter comes before the board of which I am a director in such a way as to give rise to a conflict of interest, I will alert the board to the possible conflict and make a full disclosure of the nature of the conflict. I will then withdraw from the meeting until the matter has been voted upon by the board.
9. If I fail to withdraw voluntarily from any meeting where a possible conflict of interest is presented, the Chairman of the board is empowered to require my withdrawal from the room during both discussion on and vote on the matter. In the event the conflict of interest affects the Chairman, the Vice Chairman is empowered to require that the Chairman withdraw in the same manner, and for the duration of discussion and action on the matter, the Vice Chairman shall preside.
10. If the board has reasonable cause to believe that I have failed to disclose actual or possible conflicts of interest, it shall inform me of the basis for such belief; and I will be afforded an opportunity to explain the alleged failure to disclose. After hearing my response and making such further investigation as may be warranted in the circumstances, the board shall take appropriate disciplinary and corrective action if it determines that I have failed to disclose an actual or possible conflict of interest.

I hereby certify this day of _____, _____ , that I am familiar with the Corporation's Conflict of Interest Policy and the attestations contained in this Statement and that the information I am providing in Exhibit "A" is true and correct to the best of my information.

_____ _____

Director Witness

_____

Date

CONFLICT OF INTEREST STATEMENT
EXHIBIT "A"

Title	Name of Other Business/Organization