A Family Health Team's Guide to Risk Management

Developed through the "Creating a Healthy Workplace Culture to Support Organizational Wellness for Interprofessional Family Health Team (FHT) Members" Project

Author: Patricia Fryer, RN, COHN(S), Cert HRM
            Patricia Fryer & Associates Inc.

March 2010

Table of Contents

Roles of Board Members

"The Board shall be responsible for the governance and management of the affairs of the Corporation in all things."

A Board of Directors is the governing body of a non-profit organization. The specific duties and responsibilities of the Directors are typically specified in the organization's by-laws, however, they tend to fall into a few general categories:

1. Strategic Planning:
    a. Creating or updating the vision and mission statements and strategic priorities; and
    b. Approving the strategic plan.

2. Monitoring Operations:
    a. Hire Executive Director (ED)– conduct annual evaluation, set his/her goals and objectives for the coming year;
    b. Establish policies for the overall management and operation of the Corporation including but not limited to: management of IT and patient information;
    c. Financial management – approving annual budget, ensuring systems/controls in place, establish signing authorities and submit audited statements; and
    d. Human Resources – ensure policies and mechanisms are in place for hiring of appropriately qualified staff and terminations.

3. Risk Management:
    a. ensure that the appropriate risk management mechanisms including appropriate insurance coverage, are in place in accordance with Ministry requirements and provincial legislation.

4. Accountability:
    a. Delegate responsibility and concomitant authority to the ED for the management and operation of the organization and require accountability to the Board; and
    b. Ensure organizational structure is in place that defines the roles, responsibilities and reporting relationships within the FHT.

5. Board Operations:
    a. Establish annual goals and objectives for the Board.

*Summarized from EMCFHT by-law #2009-1 and the Ministry of Health and Long-Term Care "Guide to Governance and Accountability", 2006.

Risk Management

Risk Management is *"exposure to any event which may threaten or jeopardize the healthcare agency, its clients, dependents or operations"* as defined in 1991 by CCHFA (Canadian Council on Healthcare Facilities Accreditation.

It is an administrative undertaking intended to protect the financial assets of a health care provider by assuring adequate insurance coverage against potential liability, reducing liability when untoward events to occur, and preventing events that are most likely to lead to liability.

Healthcare risk management is a comprehensive system or process through which risks to a healthcare facility and all who are served by and associated with it, are identified, classified, evaluated, and controlled to predict, limit and reduce future potential risks or losses.

The requirement to prevent and/or minimize risk to staff and patients, reputation, property, net income or the liability of the facility remains an unchanging organizational commitment in health care.

Types of risk in health care

Strategy/Governance/ Organizational/Policy risks	• Risk that the organization structure, accountabilities, or responsibilities are not designed, communicated or implemented to meet the organization's objectives. • Risk that culture and management commitment do not support the formal structures/systems/operations. • Risk that strategies and policies fail to achieve required results.
Operational (Care/Service Delivery Risks)	• Risk that services will not get completed or delivered in a timely manner, as expected. Includes business continuity risk.
Human Resources (People) risk	• Risk that capable and motivated staff will not be available to get the job done. This could be caused by resignations, turnover, inability to hire, lack of skills, strikes, injury, etc. • Recruitment/Retention (qualified workforce).
Client/Patient/Stakeholder Satisfaction	• Risk of failure to meet expectations of patients/clients, partners, the community, the broader public, other governments, ministries, etc.
Reputational/Public Perception Risk	• Loss of reputation. • Loss of confidence. • Poor public/media perception (bad press, media

	scrum). • Related consequences (e.g. loss of funding).
Patient Safety Risks	• Failure to meet Accreditation goals resulting in loss of Accreditation status (partial or full). • Risk of lawsuits from injured patients or their families.
Legal/Compliance Risk	• Risk that initiatives or actions will contravene a statute, regulation, contract or that the organization will be litigated against.
Information risk	• Risk that information produced or used, is incomplete, out-of-date, inaccurate, irrelevant or inappropriately disclosed (right to privacy).
Financial Risk	• Risk of financial losses, overspending or the inability to meet budgets and plans. • Foundation/fundraising.
Technology Risks	• Risk that information technology infrastructure does not align with the business requirements, and does to support availability, access, integrity, relevance and security of data. Includes business continuity risk.
Culture	• Accreditation places an emphasis on a positive organizational culture as the underpinning to successful management of risks/threats and continuous quality improvement.

⇒ A sample **Credentialing Policy** to reduce human resources risk is included in the package.

⇒ A sample **Disclosure Policy** is included in this package.

Quality Improvement/Assurance

Quality Assurance is an ongoing planned and comprehensive program designed to objectively and systematically monitor and evaluate the quality and appropriateness of patient care, to pursue opportunities to improve care, and to resolve identified problems.

 For risk management to become a complete and comprehensive part of the health care organization setting, the program must secure clinical staff involvement and support and must lead to human resource skills and behavior changes. The common goal of health care professionals is to improve the quality of care and, therefore, there must be successful linkage between risk management and quality of care.

In recent years the areas of overlap between risk management and quality assurance have grown. However, the implementation of quality assurance and risk management programs in health care organizations has met with some opposition, in part, because both play a role in mentoring health care delivery. In general, however, the concept of quality assurance has been considered more palatable because its techniques are tied to more specific events or incidents; its objectives are in line with those of health care practitioners; and its loss control financial considerations are not as prominent.

In contrast, risk management conjures up visions of legal action or executives wringing their hands over financial constraints.

Considerable effort is now going into designing operational structures and processes which effectively tie risk management with quality assurance and patient and staff safety, as well as with other related functions such as utilization management, safety and infection control. And thus we now are looking at Enterprise Risk Management.

Enterprise and Operational Risk Management

> *Enterprise Risk Management (ERM)* is a process, effected by an entity's board of directors, management and other personnel (all people in the organization), applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity and manage risk to be within its risk appetite, to provide reasonable assurances regarding the achievement of entity objectives.
>
> Source: The Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management Integrated Framework, 2004.

In health care, some experts are concerned that the approach to healthcare risk management and patient safety has always been too clinically focused. Some feel that ERM is too business operation focused and believe that the whole system needs to be involved, with recognition of the effect each has on the other. When the whole system is considered in relation to the management or risk, the outcomes will be much better. The support must come from the most senior levels of the organization, including the Board, but also needs to address the idea of everyone's involvement and methods of getting the knowledge to the front lines - and - learnings from the front lines.

The underlying premise of enterprise risk management is that every entity exists to provide value for its stakeholders. All entities face uncertainty and the challenge for management is to determine how much uncertainty to accept. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value.

Enterprise risk management enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value.

Value is maximized when management sets strategy and objectives to strike an optimal balance between growth and return goals and related risks and efficiently and effectively deploys resources in pursuit of the organizations objectives.

Clinical Risk Management vs. Enterprise Risk Management

Clinical Program Focus	ERM Focus	ERM Benefit
Risk Management is viewed as a department	Risk Management is viewed as a component of strategic planning	Risk management insights help the organization achieve strategic goals and further overall mission
Risk Manager is a department head	The risk management perspective is embraced at the senior executive level	Commitment to controlling loss extends from the governing board down through the organization
Risk manager focuses on clinical risks, both present and emerging	Risk manager proactively identifies and manages risks across the entire enterprise	Risks emerging anywhere within the organization are addressed early on, when damage can be contained
Risks are viewed as discrete events	Risks are viewed as interrelated and more effectively managed by an integrated, organization-wide program	Risks are managed more efficiently, strengthening the organization's finances and freeing resources for investment and growth
Risk is transferred through a variety of conventional insurance products	Risk manager is open to a wide range of strategies, conventional and alternative, for managing enterprise-wide risk	The insurance procurement process is streamlined and overall costs are reduced.

Contracts and Service Agreements

Many facilities contract for supplies or services. This may include:

> ➤ Pharmaceutical supplies;
> ➤ Equipment & maintenance;
> ➤ Computers and their maintenance;
> ➤ Construction or renovation projects; and
> ➤ Respiratory services.

In addition to formal contracts, a variety of documents may be signed such as leases, or purchase/sale agreements for products or real estate. Such documents and contracts should be reviewed by legal counsel to ensure that the wording protects the facility from undue liability.

Contracts must be carefully done. The risk manager's or delegate's principal role in contract review is not necessarily to advise about what the contract should say, but to recognize what the issues are and to make sure that the person with knowledge of those issues has had a hand in drafting or reviewing the contract.

The six (6) key elements of a contract are:

1. **Intention** by all parties to create a contract.
2. An **offer** made by one party.
3. An **acceptance** of the offer by the other party.
4. *Something of value being exchanged by each party. This is called **consideration**.
5. The **capacity** of each party to make a contract. In order to have this capacity, each party must be a **legal entity** – e.g. an individual or a corporation.
6. A **legal purpose** to the contract.

A particularly sensitive issue in hospital contracting where an outside party has access to hospital data regarding either its patients or its physicians is restricting the use of this information.

Following are examples of the types of contracts that the risk manager can review and some guidelines describing what to look for:

1. Physician contracts for services.
   The risk management review should include the following:
   - Credentialing;
   - Risk Management/Quality Assurance Program;
   - Administrative Control Issues – hiring, firing, discipline; and
   - Insurance provisions and coverage.

2. Student Affiliation Agreements

   Agreements with schools who provide education and training for health professionals such as nurses, dietitians, pharmacists place their students in FHTs in order to provide them with clinical experience. Generally, they are not "paid" under these agreements. The risk manager should ensure that there is a written contract, which should include:

   - Compliance with FHT policy and procedures;
   - Protocols for failure to observe policy;
   - Claims investigation procedure;
   - Disclaimer for loss or damage to property;
   - WSIB inclusion – procedure in the event of injury;
   - Professional liability inclusion; and
   - Health examinations for communicable diseases.

3. Equipment Contracts and Purchase Orders

   For the purchase of major pieces of equipment, the facility should have a capital equipment form for internal use that ensures that risk management and safety features have been evaluated and built into the contract with the vendor. The form should include:

   - Information supplied by the department and/or individual(s) requesting the equipment;
   - The clinical department if patient care is involved;
   - The maintenance and housekeeping departments (or site administration);
   - Central supply if that department cleans the equipment or stores chemicals and supplies used with the equipment; and
   - Any other department that uses, cleans or maintains the equipment – and, of course, the risk manager.

   Evaluation of the equipment by use of this form will bring out issues that should be covered with the vendor. Included in the form should be:

   - The warranties the FHT will require of the vendor;
   - Maintenance;
   - Upgrading protocol;
   - Confidentiality of information;
   - If leased, who insures, calibrates and maintains the equipment;
   - In-service education;
   - Shelf life, disposal;
   - Replacement parts;
   - Delivery schedule;

- Right to terminate without penalty; and
- Recalls, significant incidents, claims, suits.

Contract review can be comprehensively done in a way that will reduce fees of outside counsel if the risk manager is involved in the process. By relying on the facilities risk insurer, the risk manager has a no-cost resource in the contract review process.

Definitions:

- *Force Majeur* – "superior force" – refers to events over which a party does not have control (e.g. war, strikes, riots, etc) and which make performance by the parties under the contract either more difficult than expected, or impossible.

- *Indemnity* – refers to one party agreeing to pay damages of the other party in specific situations. This section of a contract is written to shift and allocate risk. Indemnity payments are meant to restore a party to the state they were in before the loss

- *Limitations of Liability* – is a contractual relationship that provides that in given situations, the parties will not be responsible for each other's damages or will only be responsible up to an established limit or under certain circumstances

Once the contract draft includes the terms that FHT personnel believe are necessary for the protection of the FHT, the draft can be sent to counsel if legal review is necessary. This will be much less costly, however, if the risk manager has followed a standard contract review process.

⇒ A sample **Checklist for Service Agreements** is included in this package.

Insurance

Insurance is a contract in which the insurer, for a premium paid by the insured, agrees to reimburse the Insured for loss or liability for loss on a defined subject caused by specified hazards or perils.

It is a system by which a risk is transferred by a person, business or organization to an insurance company which reimburses the insured for covered losses and provides for sharing of costs or losses among all insured.

Liability insurance indemnifies the Insured from sums they may be required by law to pay a third party as damages for bodily injury or property damage.

Common types of liability insurance include:

- General Liability: Premises, Products and Completed Operations;
- Professional Liability;
- Directors and Officers' Liability;
- Environmental Impairment Liability;
- Employer's Practices Liability; and
- Personal Liability.

There are two types of liability coverage Forms:

- *Occurrence Form* – the loss must occur during the policy period and may be reported at any time, unless there is a specified cut off period; and
- *Claims Made Form* - where the loss must occur after the retroactive date but must be reported d for the first time during the policy period

Types of Insurance:

Type of Insurance	Definition	Examples
First Party	Provides coverage for the insured's own property or person. Is intended to indemnify and restore the insured to the same financial position that they had prior to the loss.	• Fire/Property • Business Interruption • Boiler & machinery • Builder's Risk • Flood • Earthquake • Crime
Third Party/Liability Insurance	Provides coverage to a party other than the insured. Coverage is	• Professional liability • General liability (premises liability)

	intended to indemnify the third party for loss or injury caused by the insured. Involves three parties: • the insured who caused the harm or damage; • the party who is harmed; and • the insurer.	• Employers liability • Auto liability • Liability • Management errors & omissions • Environmental Impairment
Health and Welfare Insurance -	Provides coverage for an insured's employees. Coverage is intended to indemnify the employee by restoring his/her health and earnings to the level they maintained prior to the loss.	• Worker's Compensation • Health Benefits • Long and Short Term Disability • Dental • Vision • Life

Who should be insured?

- The subscriber – "named insured";
- Associated or affiliated foundations;
- Employees – but, only in the course of their employment;
- Directors, officers, trustees, committees and members of such boards and committees;
- Persons, firms or corporations financially controlling or controlled by the "named insured";
- Volunteers and auxiliaries;
- Students – but only for work under the supervision, direction or instruction of the placement (hospital, FHT);
- Social clubs sanctioned by the named insured;
- Physicians, dentists, interns, residents and midwifes but only for performing administrative duties for the insured; and
- Medical personnel (excluding physicians, dentists, interns, residents, and midwives), scientific staff and technicians while engaged in research or contract work for the Named Insured regardless of source of remuneration.

What should be covered?

- Bodily injury (including personal injury);
- Advertising liability;
- Property damage;
- Professional liability;
- Blood transfusion legal liability;
- Contingent employer's liability;
- Employee benefits liability;
- Errors and omissions liability;
- Environmental impairment liability;
- Non-owned automobile liability;
- Crime insurance; and
- Property insurance (could be separate from liability insurance and a different carrier).

Other things to consider:

- Retroactive Coverage;
- HIV/AIDS Supplementary plan;
- Tenant's legal liability; and
- Host liquor liability.

Drafting Coverage Specifications

The process should begin at least six (6) months before policy inception. The first step is an evaluation of exposures and the insurance products available to cover the exposures. Once the exposure(s) to be transferred are identified, an application for coverage is prepared. This application is often called an underwriting submission. The submission serves as a tool to present the organizations business strategies, risk exposures and insurance desires to the insurance marketplace.

Most carriers have a standard format. The submission is then submitted to the carrier's underwriting department and a quotation is developed.

Components of the underwriting submission may include:

- A description of operations and organizational chart;
- Listing of named insured and additional insured;
- Retroactive dates (if coverage is on a claims-made basis);
- Location listing;
- Current and historical exposure information;

- Currently valued historical loss experience (five to twenty years of loss experience);
- Large loss details for any claim over $100,000;
- Signed application;
- Current annual report or other financial statements;
- Description of risk management department procedures including loss prevention, quality improvement, patient safety initiatives and claims management;
- Current actuarial report;
- Accreditation report; and
- Description of desired coverage – limits, deductible, coverage extensions, underlying coverages, pricing guidelines, policy period, key coverage terms or services.

Identifying the carriers who are interested in assuming the organizations risk is the next step.

Key criteria to consider when selecting a carrier include:

- Does the purchase of this policy support the short-term or long-term objectives of the health care organization and the risk management department?
- Is the insurance carrier finically secure?
- Is the carrier knowledgeable in health care operations?
- Is the carrier flexible?
- Is the pricing competitive?
- How will future pricing be affected by the organizations' favorable or unfavorable loss experience?
- How will future pricing be affected by losses within the health care industry or outside of the healthcare industry?
- Is the carrier capable of meeting the claims administration, loss prevention, clinical risk management, risk management information systems and educational needs of your facility?
- How long has the carrier been offering this type of coverage and what is its past history in the marketplace?
- What is the carrier's claims handling philosophy? Will it allow input from the organization?
- Who does the carrier use for legal counsel?

Once quotations are received, they should be analyzed for price, terms, services and other qualitative issues. Insurance policies vary in terms and conditions but key coverage considerations should include:

- Is the quotation based on complete and accurate exposure and loss information? If not, could the pricing change based on outstanding data?

- What are the limits of the policy? How do they apply?
- Is there a deductible or retention and how does it apply?
- Does the policy include a co-insurance provision?
- What is the policy period, effective date and expiration date of coverage?
- What is the premium?
- Is coverage claims-made or occurrence?
- If coverage is claims made – what is the retroactive date?
- What is the intent of coverage?
- What are the key exclusions?
- Who is covered by the policy?
- What is the coverage territory?
- What is the procedure for reporting claims?
- What is the definition of a claim?
- What is the timeframe within which claims must be reported and who must report claims?
- How are defense costs handled?
- Are there provisions for adding or deleting exposures during the policy period?

Once coverage has been bound, it is helpful to have the broker or agent prepare an insurance summary that emphasizes key components of your insurance policy. It will include a description of the type of policy purchased, policy numbers, policy period, limits of coverage, deductibles, premiums, a coverage overview and major exclusions. Another helpful tool is a schedule of insurance which is a condensed version of all insurance coverage and can be used as a quick reference guide.

Occupiers Liability

The Ontario Occupier's Liability Act defines the term "occupier" as a person who is in physical possession of a premises or a person who has responsibility for and control over the condition of a premises even if there is more than one occupant.

Definition of Occupier:
- A person, company or other entity that owns the premises, has possession of it or has responsibility or control over it; and
- All parties that have an interest in a property (property owner, landlord & tenants) can be considered occupiers.

Occupiers Duties:

- Persons using the premises must be kept reasonably safety from harm.

The occupier's duty is to take such care, in all circumstances that are reasonable, to ensure the reasonable safety for those people entering onto the premises. It is important to note that the standard the occupier needs to achieve is one of "reasonableness", not a standard of perfection. What is reasonable is very dependent upon circumstances, which is why every case is decided upon its own unique set of facts. For example, if there is a blizzard, it is not reasonable for the occupier or the owner of the property to shovel the snow away every five minutes. However, if the blizzard comes to an end and the snow and ice are left on the travel portion of the sidewalk for two days before it is removed, then that is very likely to be considered unreasonable. The occupier has a duty to remove the snow within a reasonable time frame and in a reasonable manner.

Duty of Care – Test

- Was the danger foreseeable?
- Was the occupier's conduct in accordance with acceptable standards of practice?
- Was there an adequate system of inspection in place and carried out?
- Was the hazard allowed to exist for an unreasonable amount of time?
- How easy would it have been to prevent the hazard?

How to limit liability - Identify and eliminate hazards:

- Ice and snow that has not been cleared;
- Unexpected elevation changes;
- Uneven surfaces;
- Slippery surfaces;
- Missing or loose handrails on stairs;
- Debris on walking paths;
- Inadequate lighting; and
- Inspection and maintenance policy and log.

Common insurers:

- HIROC – Healthcare Insurance Reciprocal of Canada (www.hiroc.com)
- Stevenson and Hunt (http://www.sthunt.com/index.html)
- Integro Insurance Brokers (http://www.integrogroup.com/en/index.html)
- Frank Cowan Company (www.frankcowan.com)
- Marsh (www.marsh.ca)

Privacy

Detailed privacy legislation and requirements are available at www.ipc.on.ca which includes:
- Personal Health Information Protection Act 2004
- Disposal of Information RSO 1990 Reg 459
- Mini Guide to Ontario's Freedom of Information and Protection Act
- Best Practices – Circle of Care

Definitions:

Privacy – is our fundamental right to control information about ourselves (including the collection, use and disclosure of that information.

Confidentiality – is our obligation to protect personal information in our care, to maintain its secrecy and not misuse or wrongfully disclose it.

Personal Health Information – is defined under the Personal Health Information Protection Act to mean certain information about an identifiable individual (whether oral or recorded) such as the individual's physical or mental health, the provision of health services or payments or eligibility for health care (among other things).

Key Privacy Terms

PHI (Personal Health Information) is "identifying information" collected about an individual. It is information about an individual's health or health care history.

      e.g. Physical/mental condition, health-card #

HIC (Health Information Custodian) is a listed individual or organization under the law that has custody or control of personal health information because of their duties.

      e.g. healthcare facilities, practitioners

Agents (PHIPA) is any person who is authorized by a HIC to perform services or activities on the IC's behalf

      e.g. contract staff or services

On April 4, 2000, Parliament passed Bill C-6, now known as the *Personal Information Protection and Electronic Documents Act*. Bill C-6 subsequently received Royal Assent on April 13, 2000. There was almost two years of debate centered on the concerns that key health care stakeholders expressed as to the possible implications of the Act on the health system. The legislation is complex and sometimes confusing. The Act provides individuals with a right to privacy concerning their "personal information" and that it should not be collected, used or disclosed without the prior knowledge and consent of the individual concerned.

Personal Information is broadly defined in the Act as "information about an identifiable individual, with the exception of the name, title or business address or telephone number of an employee of an organization". It includes such things as race, ethnic origin, color, age, marital status, religion, education, medical, criminal, employment or financial history, address and telephone number, numerical identifiers such as the Social Insurance Number, fingerprints, blood type, tissue or biological sample and views or personal opinions.

The Act also includes a separate definition for personal health information – for an individual, whether living or deceased.

Personal Health Information means:

- Information concerning the physical or mental health of the individual or any health service provided to the individual;
- Information concerning the donation by the individual of any body part or any bodily substance or information derived from the testing or examination of a body part of bodily substance;
- Information that is collected in the course of providing health services to the individual; and
- Information that is collected incidentally to the provision of health services to the individual.

The majority of health care facilities' activities are unlikely to be subject to the Act since they are operated on a not-for-profit basis and are generally understood not to be commercial. Information disclosures made between a healthcare facilities and a private sector organization such as a private nursing home, laboratory, pharmacy, or clinic are likely caught by the Act.

Ten Privacy Principles

1	Accountability	Organizations are responsible for the personal information under their control. A specific individual or position must be designated as responsible of the organization's compliance with the Act.
2	Identifying Purpose	Organizations must advise individual why they are collecting the personal information and how it will be used.
3	Consent	Organizations will be required to obtain an individual's consent to collect, use or disclose personal information, unless they can satisfy one of the limited exceptions to obtaining consent. Consent may be implied or expressly given; it may be provided orally or in writing
4	Limiting Collection	Organizations will only be entitled to collect the minimum personal information necessary to fulfill their stated goals.
5	Limiting Use, Disclosure or Retention	Organizations must use and disclose personal information in accordance with the reasons stated to the individual. New uses and disclosures require new consent. Also, the information should be kept only for as long as necessary to meet the original purpose.
6	Accuracy	The information must be kept accurate and as current as necessary to fulfill the stated purpose.
7	Safeguards	Organizations must safeguard individual's personal information to protect against loss, theft, unauthorized disclosure, copying, use or alteration. Technological safeguards include the use of passwords and encryption of information. Organizational security measures include the use of security clearances and limiting access on a "need to know" basis.
8	Openness	Organizations must inform individuals about the personal information they hold, the purposes of which it is used, the persons to whom it is disclosed and how an individual may access it.
9	Individual Access	Individuals are entitled to be given access to their personal information retained by organizations to ensure its accuracy and completeness, and to identify to whom it was disclosed, subject to certain exceptions.
10	Challenging Compliance	Individuals can challenge an organization's compliance with these principles both through the organization's required complaints process and by making a complaint to the Privacy Commission. When the Privacy Commissioner investigates a complaint or conducts an audit, the Commissioner has broad powers including entering an organization's premises, interviewing people and extracting records.

The Ontario Ministry of Government Services has also developed a variety of privacy tools to identify and resolve privacy issues. Tools include Privacy Impact Assessment guidelines and Electronic Service Delivery Privacy standards. They can be found at: http://www.accessandprivacy.gov.on.ca/english/index.html.

The Ontario Information and Privacy Commissioners' Office has also produced diagnostic tools for assessing and improving the level of privacy within organizations. They can be found at: http://www.ipc.on.ca/english/Home-Page/.

Legal Claims

Claims Management – What is it?

> *"A systemized approach to reducing the Financial loss and negative community image of a healthcare organization in situations where prevention fails and injury occurs"*
>
> Ref: Risk Management Handbook for Health Care Organizations: Volume 3; 5th edition

The following is about claims and litigation management issues related to a medical professional and general liability program. However, the concepts and principles also pertain to other exposures in the healthcare setting including employment practices liability, directors and officer's liability, fidelity and fiduciary liability.

Claims and litigation management most fittingly belongs in the operational-clinical risk domain for two (2) reasons:

- The risk in this domain derives from an organization's core business practices, which rely on systems, practices, and people. "Medical professional liability" arises from the delivery of health care and the practice of medicine by professional caregivers who adhere to specific standards of care.

- Claims and litigation management best practices derive from reliable systems, collaborative practices, and communication between and among health care providers and claims and litigation managers.

The health care organization and those individuals who represent it can directly affect the dollars paid in claims by the manner in which they administer claims.

Basic claims management principles apply, regardless of the nature of the health care organization.

All claims should be handled in a fair and equitable manner; that is, valid claims should be settled promptly and for a reasonable amount; frivolous claims should be vigorously defended.

The role of the person responsible for managing claims (claims managers) will vary, depending on the nature of the healthcare organization and its' insurance program. If the organization is commercially insured, the claims managers' role is to monitor the activities of those with hands on responsibility for claims management.

The management of claims involves the following key steps:

- Notifications;
- Claims Identification;
- Claims reporting;
- Claims and potential claims files;
- Claim Investigation;
- Claims Management Strategy;
- Settlement; and
- Litigation.

Notifications

Communicate with the necessary people and document the communication.

- Report the event to the insurance carrier;
- Notify the attending physician if that physician is not already involve in or aware of the event;
- Notify senior management as appropriate;
- As appropriate, notify the coroner; and
- Notifying the named individuals (other than the physician(s)…other professional staff, anyone else named in a Statement of Claim, in a complaint letter, etc.).

Claims Identification

The organization's risk management plan should include a system for identifying and reporting actual AND potential claims to the person responsible for claims management.

> *"Risk Identification is the process through which the person responsible for claims management becomes aware of risks in the health care environment that constitute potential loss exposures for the institutions."*
>
> Such exposures can include:
> - Loss of financial assets;
> - Casualty losses to property;
> - Human losses through death/injury of employees; and
> - Intangible losses to public image and reputation.

Identification of Potential Risks and Potential Compensable Event

There are many information sources to identify potential risks.

- Incident reporting, in which employees report accidents and occurrences not consistent with normal operating routines or expected outcomes – including near misses;
- Patient/family complaints and satisfaction survey results;
- Prior medical professional liability, property and casualty and workers compensation claims data;
- Surveys by insurers and claims history;
- Contracts, leases and other agreements entered into by the facility;
- Information generated through the facility's infection control and performance improvement functions;
- Communication and informal discussions with staff within the facility; and
- Notification through other means (i.e. news article, etc.).

Staff of the health care facility should be provided with ongoing education regarding trends in medical professional liability litigation and insurance coverage, reporting of events and other related topics.

If any health care provider or administrative personnel receive letters of representation, demands for damages or formal legal papers, they should immediately send such notices to the person responsible for claims management who will forward them to the insurers.

Potential Compensable Event

A Potential Compensable Event is any incident where there is neither an active claim nor any formal legal action. It includes cases in which an unexpected event caused injury or potential injury and can include denial of treatment. Usually there is some expression of dissatisfaction or "perceived" injury. It can include certain events that, in the opinion of the risk management, can give rise to a demand for compensation or a lawsuit.

The following Emergency Guidelines can help staff deal with these types of events:

- DO NOT delay prompt patient care.
- Be tactful; open an honest with the patient and family members regarding the situation. Only reveal FACTUAL information known.
- Provide objective information to help them understand what has happened and what action will be taken.
- Document the incident in a timely fashion.
- Notify your supervisor immediately.
- Complete an incident report.

- Notify the person responsible for claims management or delegate as soon as practicable.
- Sequester all evidence (medial records, medication packaging, disposable equipment, etc) even remotely relate to the incident.
- Do not "finger point" or "blame"
- Do not discuss the incident with anyone other than a supervisor or person responsible for claims management.
- Do not make any promises to the family.
- Say "I'm sorry" if the circumstances warrant it – BUT only after discussing with the person responsible for claims management or legal counsel. You are not apologizing for possible negligence, rather for the fact that the incident occurred.
- Treat the patient and family with dignity and respect.

$\Rightarrow$ A sample **Checklist for Legal Claims** is included in this package.