LAW ENFORCEMENT LIAISON COUNCIL
SPRING/EARLY SUMMER 2013 LELC NEWSLETTER EDITION

Partners!

LELC: OPENING REMARKS

The spring/early summer edition of the LELC Newsletter has plenty to offer from public/private partnership information, concepts in risk management, preparedness issues, and cyber risk. Please take a few moments from your busy schedules to enjoy insightful articles presented by ASIS LELC members!

Operation Partnership Emergency Network
Submitted By: Mr. John Joyce, Member of the Law Enforcement Liaison Council, IACP Committee & Major Billy Cordell, Fort Worth, Texas Police Department

The City of Fort Worth's departments of public safety and private sector's security groups have enjoyed good working relationships for the past two decades. These relationships strengthened in 1993 when the Operation Partnership Security network was formed. The program was developed from a Seattle Police Department program and operates as a link between the police and private security. Operation Partnership's objectives are to share crime information, provide training at monthly meetings and establish a communication network via a fax system. Operation Partnership has advanced in technology through e-mail based distribution lists and continues to build upon the strong relationships established years ago. Continuing that tradition, Fort Worth public safety officials, members of the Building Owners Managers Association (BOMA), and local security directors initiated dialogue concerning the need to enhance the mitigation, response, and recovery from a crisis or disaster in July 2001.

Fort Worth is no stranger to critical incidents. In 1995, a large hailstorm struck without warning during a major public event causing several serious injuries and vast amounts of property damage. In 1999, a lone gunman entered a church during a youth event and

LEADERSHIP 2012/2013

Chairperson:
Mr. Brian Reich, CPP

Vice-Chairperson:
Mr. Briane M. Grey

COMMITTEES:
(Chairpersons)

Executive Committee
Mr. Tom Conely, CPP
Mr. Bernard Ferguson
Mr. Mahbub Choudhury

Annual Seminar
Mr. Michael D. Gambrill

Book Review
Mr. James Brown, CPP

Council Certification
Mr. Paul Sweeney, CPP

Guidelines Committee
Mr. Mark Riesinger, CPP.

Interpol Committee
Mr. Carlos Velez

Membership Committee
Mr. Mark Riesinger, CPP

Publications Committee
Mr. Robert Lee

Session Reviewers
Mr. Robert F. Graham, CPP

Subject Matter Experts
Mr. Ira S. Somerson, CPP

School Safety&Security
Mr. Mark Wasylyshyn

Transitional Training
Ms. Stacy Irving

Web Master
LT. Mark Competello, CPP

IACP
Mr. James (Tom) Roberts, CPP

murdered eight people including himself, and injured seven others at the event. In March of 2000 a destructive tornado struck the Central Business District causing five fatalities prompting 450 million dollars in property damage. In the aftermath of these tragedies, a committee of interested constituents of the public and private sectors combined efforts to form the Operation Partnership Emergency Network, or OPEN.

The original OPEN committee consisted of members of the Fort Worth Police and Fire Departments, members of Operation Partnership (Security Network), the Building Owners and Managers Association (BOMA), Downtown Fort Worth Inc. and the Federal Protective Services. This group of dedicated individuals met weekly to develop a mission statement, by-laws, and an emergency communication system that was unprecedented. The committee identified several vital organizations from the public and private sectors as critical components of OPEN and brought them to the table. In February 2002, OPEN was announced by the Mayor of Fort Worth as an emergency communications system established to disseminate critical information in a timely manner to business operators in the Tarrant County, Texas area.

The Operation Partnership Emergency Network's mission is: "to develop and enhance emergency response systems, procedures, and training programs, which will facilitate the emergency response and recovery capability and awareness of affected business owners and operators in the event of a crisis response situation". In addition, it is a goal to continually evaluate the crisis response and training needs of the membership and develop systems that meet those needs.

OPEN's objective was to utilize the technology that business has available such as, text messaging and emails to accomplish its communications goals without requiring membership dues to its benefactors. The first priority was to establish a communications network that provided an early warning system of an impending crisis or when a pre-emptive message was not possible, provide the membership with information at the onset of a crisis. Many individuals carry cellular telephones capable of receiving e-mail or text messages. OPEN uses these devices as a conduit for providing timely and critical crisis information to the membership. Members submit their e-mail address and cellular numbers, which is entered in three separate databases. The City of Fort Worth maintains two databases and the third database is maintained by City Center Security, (a private security group with property in downtown Fort Worth) on a completely separate system. This system affords OPEN the ability to have a back-up system should the City's computer system fail. The use of mobile devices ensures that the emergency information is transmitted to a person, regardless of where they are at the time of the incident and they can begin a rapid response based on their business needs. Weekly tests of the system are sent out to the membership, which provides familiarity and reliability measurements.

A website was established, (www.operationpartnership.org) to provide useful information concerning OPEN and updated information during prolonged critical incidents.

After the communication network was established, the second priority of OPEN was to address complications that arose from perimeter access issues. The private sector has millions of dollars invested in their businesses and had strong concerns that they were not permitted inside the perimeter in a timely manner when a crisis occurred. The OPEN committee agreed that a system should be developed including individuals from the private sector who had a vital interest in the incident. Another accolade of OPEN was the creation

of a perimeter access procedure, which utilizes a color-coded system consistent with Homeland Security's color-coded system, (blue, yellow, orange, and red).

The City of Fort Worth, like many cities, operates under an Incident Command structure. Within that system, an Incident Commander is in charge of the overall incident management and makes decisions based on input from support personnel. OPEN identified the Building Owner or Manager, Director of Security, and the Chief Engineer as important personnel in the private sector who could benefit by becoming a partner in the Incident Command structure. During a critical incident the incident command requires information about specific properties that these individuals can provide. In addition, public safety resources are strained during a major event and these individuals can provide support for non-dangerous tasks such as building searches and damage assessments. Public Safety also realized these individuals play a critical role in managing and recovering from an incident involving their organization and as such, are permitted to apply for a pre-issued access card. Upon approval, these individuals are issued a pictured ID card that identifies their affiliation with OPEN, operational title, and property address. During a critical incident these individuals are given prompt access to their areas when they present their badges at a secured checkpoint. Individuals receive a specific color-coded badge based upon their need to enter a secured area, which is dictated by the position they hold in their organization. For example, red-access permits access to public safety and emergency responders only. Orange-access permits access to building owners, managers, security directors, and chief engineers. Yellow access grants access to another group of individuals and so on. A system was also established that assigned a public safety liaison to specific quadrants of the secured area. The liaison's responsibility is to interface with individuals who have business interests in the quadrant. The liaison has the authority to issues access passes (self-destructing badges) to individuals or vehicles that have a legitimate reason to enter the area. The liaison also serves as a conduit of timely information to the property owners in the area and direct communication with the Incident Commander. One of the major frustrations realized during the tornado of 2000 was that public safety was overwhelmed with requests and inquiries and was not able to effective accommodate the requests for information. Another frustration was that property owners were not able to get workers, contractors, or supplies to their businesses to begin the assessment and recovery process. Through OPEN's access control program, (the ID badges, self-destruct access badges, vehicle passes, and the liaison officer) these concerns will be eliminated in the future.

Finally, OPEN, through its charter, established a training component. The initial training session offered the membership insight into the operational procedures of the Fort Worth Police and Fire Departments during a crisis, an overview of the OPEN system, introduced the perimeter access control system, and presented a short scenario recreating a crisis in a business environment. This training session was the precursor to formal tabletop exercises, which tested the membership's disaster planning and preparedness skills and knowledge. It is known in professional circles that effective training is a critical component to successful disaster mitigation, response, and recovery. Typically, private security is offered training programs through private enterprises who focus on disaster planning or through federal, state or local agencies who offer this training as a service.

OPEN has strengthened the relationship between the public safety departments and the partnership that exists with the private sector businesses. Because of OPEN and its partners, the City of Fort Worth and those who are members of OPEN, are better-prepared and more informed in matters of crisis management. Additionally, the early warning system of text messaging and email notification to OPEN members is providing a benefit never

before realized in the private sector in our region. Through OPEN, the City of Fort Worth is better prepared to respond to and recover from critical incidents.

For more information please visit the website at: www.operationpartnership.org.

Understanding and Assessing Risk
Submitted By: B. Bernard Ferguson
Member of the Law Enforcement Liaison Council, Executive Committee

Organizational leaders are required to constantly make decisions where they must select the best option from among several alternatives. Because it is virtually impossible to obtain one-hundred percent of the information surrounding a particular situation, organizational leaders are often faced with having to decide with the understanding that their decisions will contain an element of unknown risk. Through the routine act of delegation, organizational leaders are assuming a certain level of risk by no longer being in total control of situational outcomes however, because of the enormity of tasks required for an organization to be successful, organizational leaders must relinquish control of certain aspects of business operations, and trust that those individuals empowered to carry out functions do so in support of organizational objectives.

Risk is an essential component of business decisions. Accordingly, simply not knowing all there is to know about a given situation when it comes to making a decision equates to risk that must be effectively managed to guard against catastrophe. Moreover, when dealing with risk, it is important that organizational leaders first consider the source of the risk as well as the probability of its occurrence. An important consideration in the risk management process involves assessing the potential financial costs to the organization to mitigate the risk when compared to simply establishing contingencies to pay for damages arising from worst case scenarios should mitigation costs prove to be cost prohibitive. Other steps include an evaluation of stakeholder impact, the probability of the risk occurring, documentation of risk findings, and continuous follow-up after the implementation of risk management strategies.

Sources of risk:
The vast majority of risks organizational leaders might encounter are either posed by humans or the result of natural causes. In either case, these risks have the potential of influencing decision outcomes. Organizational risks are identified through numerous methods including personal observations, listening to others, and asking questions.

Stakeholder impact:
Assessing the impact of downstream consequences the potential risk places upon the organization's stakeholders is a critical element in risk assessment. Organizations suffer when leaders are not attuned with the feelings of their employees relative to potential risk exposure particularly when such neglect result in lower employee morale and diminished work performance.

Estimation of risk probability:
The probability of the worst case scenario ever materializing occasionally weighs on whether or not an organization is willing to expend financial resources on mitigating the risk. Another factor in risk assessment involves an organization's risk appetite, where those organizations that are risk averse are likely to be the most conservative when it comes to exploring options that deal with unknowns.

Evaluate feasibility of mitigating risk:
Organizations will not be successful in mitigating all of the risk they are susceptible of facing, and although risk is a condition that has an impact on project outcomes, it is not always financially feasible to make an attempt at mitigating certain risks. For example, risks with a low probability of occurring, or those that do not overly expose the organization might not rate immediate action.

Document and disseminate findings:
Maintaining a written record of risk identification and/or abatement is a critical component of risk management. Because of the potential liabilities associated with organizations having to defend its risk management process, particularly in situations where risks materialized after the organization was made aware of the potential outcome but instead chose not to mitigate the risk. Sharing appropriate documents relative to organizational risk management with stakeholders is also an element of an effective risk management program.

Provide risk assessment follow-up:
After the risk has been documented following its identification whether or not it was actually mitigated, continuous follow-up is important to monitor results of mitigation, or determine whether or not the current state of the risk has risen to a level requiring intervention. An effective process for tracking both potential and known risks following the implementation phase not only allow organizational leaders to better plan for contingencies, but enable them to devise effective strategies for maneuvering through the unexpected challenges risk poses for organizations.

5 step risk assessment process:

- Classify the problem
- Assess vulnerabilities
- Decide on the right course of action
- Implement the plan
- Continuous evaluation

Public/Private Partnership: The National Business Emergency Operations Center
Submitted By: Mr. Raymond C. Ferrara, CPP
Member of the Law Enforcement Liaison Council, Newsletter

Uncertainty and Risk will continue to either challenge or provide great reward for business enterprises. Companies will continue to face natural disasters and manmade tragedies. It doesn't matter which profession you represent: emergency planner, risk manager, business continuity planner, security manager, or health and safety professional. Are you driving your business on the road to resiliency or the pathway to extinction? Resilient businesses are postured to thrive no matter what the circumstance provides. Successful businesses are built on the concept of accomplishment. Resilience is about believing your organization is structured and solid enough to be here today, tomorrow, and ten years from now. A great new public/private partnership, the National Business Emergency Operations Center (NBEOC) is a groundbreaking new virtual organization that serves as Federal Emergency Management Agency (FEMA's) clearinghouse for two-way information sharing between public and private sector stakeholders in preparing for, responding to, and recovering from disasters. In a crisis, close collaboration between the FEMA and the private sector is critical to protecting citizens and rebuilding communities.

NBEOC Design:
Facilitate a public-private sector exchange of information about needs and capabilities.
Support the ability of state, local, and tribal governments to recover from disasters by connecting them with FEMA's regional private sector liaisons and the NBEOC's national network of resources.
Foster cooperative and mutually-supportive relationships that eliminate duplicative partnership development efforts.
Assist Regional and Joint Field Office (JFO) partners in identifying where support is available or needed to restore business operations to the affected areas.
Engage key stakeholders who bring resources, capabilities, and expertise to bear during disaster response and recovery efforts to determine impacts on their ability to provide services to the public.
Improve situational awareness across the affected areas.

NBEOC Membership and Structure:
Participation in the NBEOC is voluntary and open to all members of the private sector, including large and small businesses, associations, universities, think tanks, and non-profits. Organizations interested in joining or sharing ideas can contact FEMA-PSR@dhs.gov.
All participation and coordination is virtual – via conference calls, email, and web platforms - with only NBEOC leadership serving in a physical capacity at FEMA Headquarters. This is reflected in the NBEOC's structure: The Director of FEMA's Private Sector Division, Office of External Affairs, has overall responsibility for the NBEOC.
FEMA's current Private Sector Representative serves as the NBEOC Director, supporting the Private Sector Division Director and coordinating the collaboration of the members.
Members are organized into groups by their affiliations, including federal partners, private sector organizations and associations, PSR program alumni, private sector functional areas, and regional/state/local organizations.
As the NBEOC grows, its structure will remain fluid, evolving to reflect feedback from participants and audience members as well as lessons learned from events and exercises.
For additional information on the NBEOC follow this link: http://www.fema.gov/private-sector.

Cyber Security Needs Increase
Submitted By: Mr. James Brown
Member of the Law Enforcement Liaison Council, Book Review Chair

Cyber security is increasing becoming a major concern, particularly for business and government. Attacks for criminal and malicious reasons are a major problem; however, they are being eclipsed by nationless states and criminal governments on a global scale launching attacks that are approaching open electronic espionage and acts of war. It is increasingly apparent that the aim of the attacks is to disrupt the government and its military capabilities, along with inflecting far reaching economic harm. Every major area of civil activity is at risk from disruptions to commerce and critical infrastructure.

The cyber economic and national security threats also create an opportunity for private security to specialize and expand into this area as either internal or external expert resources to government and business. The federal government has started regulation efforts and Congressional legislation is likely in the future. *Bloomberg Law* [1] reported there

were 513 filings by lobbyist in Washington, D.C. concerning cyber security, as industry, finance, utilities, transportation, and others vie to influence regulation and legislation.

From a somewhat new direction, law firms are increasingly offering cyber security services. The *Wall Street Journal* reported[2] that in some cases, clients are advised to hire a lawyer first, and then the lawyer hires a cyber forensic company to maintain confidentially. Law firms can provide "client-attorney privilege" and the confidentiality it confers. Lawyers can also provide advice on how to handle issues with potential liability, such as a data breach by cyber attack that has the potential to result in a class action lawsuit. In 2011 the average company data intrusion costs 5.5 million dollars[3]

1April 5, 20013 interview with David Ransom of McDermont, Will and Emery
Wall Street Journal [2] Law Firm Tout Cybersecurity Cred, April 1, 2013 B1
[3] Ibid

Is a covenant convenient to underline partnership in the Health Care Sector?
Submitted By: Mr. Mike Van Drongelen, CPP, PSP, PCI
Member of the Law Enforcement Liaison Council, School Safety & Security, Interpol

History of the covenant:
In the Netherlands and in many counties alike, the health care sector and police have regular interactions. Both parties struggle with the same issues and at times have conflicting interests. One example is when police need information about patients admitted to a hospital or other health care facilities. Because police requests for information on patients can be for different reasons, such as assisting civilians or solving offenses, clear and solid agreements were needed to find common ground. In 1998 the regional police force, the Public Prosecution, and the health care sector in the Amsterdam region of the Netherlands admitted that the interests and responsibilities of both the criminal justice system and health care organizations were not always parallel to each other. Furthermore they concluded that all parties are dealing with a wide range of laws, which are not always properly aligned. In practice this lead to ambiguities and misunderstandings. To counteract these ambiguities and misunderstandings all parties involved drafted a covenant and an informative guide for a number of common situations. The goal of this covenant and informative guide is to seek a method to do justice to everyone's position without compromising everyone's statutory powers and responsibilities. On 28 October 1998 the covenant, which was prepared by a workgroup of experts from hospitals, healthcare institutions, ambulance services, the Royal Dutch Society for the promotion of Medicine (KNMG) the regional police force, and the Public Prosecution of the Amsterdam region, was signed to provide a solid foundation for a partnership in the Health Care Sector.

Putting the Covenant and Informative guide put to practice:
After signing the covenant in 1998 all parties involved appointed a contact officer available on a 24/7 basis and agreed all contacts between the institutions will pass by the contact persons. Furthermore all employees of the institutions involved were given an informative guide to provide guidance on subjects such as professional secrecy, providing (medical) information, visiting and interrogation of patients, the detection of narcotics, weapons and ammunition, access to health care institutions, guarding of patients, seizure of goods, blood

tests, no conviction of natural death, sexual offenses, child abuse, workplace violence and medical staff suspects. In the following paragraphs these subjects are further explored.

Professional secrecy:
Professional secrecy is based on the idea that the patient should have free access to assistance without having to fear that his data will be disclosed to the third parties. The confidentiality of the employee, derived from all members of the relevant organization, is a right of the patient and covers everything the employee knows about a patient in the context of exercising his duties. The employee should also be silent about the fact that a person is present in the institution, the personal data of the patient (name, date of birth, etc.), the fact that clothing is torn or information about the attendants / visitors of the patient. Only under certain conditions, the silence will be broken. Even if the patient gives permission to provide its data to third parties, the employee must independently decide whether this data will actually be provided. Only in exceptional circumstances the professional secrecy can be broken without the patient's consent. It is up to the employee to weigh whether he should break confidentiality. Requests for information about a patient always run through the contact officer of his / her organization. Ultimately, the issue of whether or not data is submitted can be brought to court. Professional secrecy is therefore one of the main reasons for the agreement of a covenant that if the police want information, the police staff does not directly approached hospital staff, but the police liaison officer. He or she then contacts the hospital liaison officer. The hospital liaison officer then approaches the employee(s) and reports to the police contact officer.

Providing (medical) information:
In the context of investigations by the police, (medical) information can be provided by hospitals and other health care institutions. The main rule is that the employee will not provide any information to third parties (including the presence or absence of someone). If the identity (name, first name, address, date of birth, residence and domicile) of the patient is not known to the police, the employee may not provide this information to the police without the consent of the patient. Regarding a request for medical information applies that if the police is aware of the identity of the person concerned, the police liaison officer‘s request may be made aware on the medical condition of the patient. This requires consent of the patient. The issue of a medical certificate on the injury of patients seen at the emergency room is not a task for the physician. After reporting a crime to the police, the victim is referred by the police to the clinic of the forensic doctor, who will send his injury statement (with the consent of the victim) to the police. For the subsequent provision of information on the nature of the injury and the health status of patients who are (were) in the hospital, the ‘medical information application’ is used by the Department of Justice which has been drawn up in consultation with KNMG. In the context of rescue activities (medical) information can be provided to the police. In the case of an unknown patient who is unable to reveal its own identity, nor to give permission to share data with the police and when that in view of the condition of the patient and/or in the context of the treatment is desired, the police liaison officer can be asked to assist in determining the identity of the patient's family to inform and involve the treatment via the hospital liaison officer. If the police are involved in an emergency admission (e.g. after an accident) the police notify the family. Optionally, the institutions’ liaison officer can be helpful. Here is an example, by requesting the present patient representative and /or family to contact the police department or a police officer. In this case the health care institution informs the family of the patient. Coordination with the police is recommended, especially in situations where police is involved with the emergency admission.

Visits, interviews, interrogation and arrest:
In the context of interviewing, interrogation and arresting patients by police, special care is needed in the coordination between the police and the health care institution. When the police want to visit a patient, whose identity and presence in the health care institution by police is known, to interview the patient as a victim / declarant / witness of a crime, they contact the c the health care institution's liaison officer to adjust their visit on the condition and activities of the patient. Via the liaison officer the most appropriate time is mediated. The patient can indicate that he/she does not want to talk to the police. If the physician considers that it is not medically justified that a patient is visited by the police, it is postponed for that moment. The police have statutory powers to interview and/or to arrest. If the police wish to proceed with the interview and /or arrest of a person that is admitted as a patient at a health care institution, the police need to know in which institution the person is admitted as well as the identity of this person. The identity of the person cannot be disclosed by the health care institution. An exception to this rule is when the police is at the scene of the crime or is present during an incident and resigns to provide medical care by medical staff. In this case the police can invoke its criminal law powers which they originally had afterwards. If the police want to use this power, they need to contact the health care institution's liaison officer as soon as possible. If the police believe that questioning during the patient's stay in the health care institution is immediately necessary, they will contact the institution's liaison officer. The contact officer of the institution asks the doctor whether it is medically justified for the police to approach the patient for questioning. The patient does not have this medical discretion. If the treating physician thinks it is medically not responsible to have the patient questioned by the police, he will notify the police via the contact officer of the institution. The health care institution is not an unusual building subject to exceptions for questioning or arrest of persons. The police may enter the health care institution upon identification to arrest anyone on the premises. If the police wish to proceed to arrest a patient, the police need to contact the health care institution liaison officer. The liaison officer consults with the attending physician on how the detention can be exercised in a medically responsible manner. Depending on the condition of the patient, the detention will be implemented at:

a) The police station, detention center or penitentiary hospital. The health care institution liaison officer makes the necessary arrangements with the police liaison officer.
b) The health care institution. If the patient cannot be transported, the patient shall be put into the custody at the institution. The medical doctor remains responsible for the patient. The police will provide for adequate guarding of the patient. If the detention is lifted, the hospital's liaison officer will be informed by police.

The police will only proceed to arrest a patient who is receiving treatment from ambulance care providers if:

a) the patient treatment is finished and he/she will not be transported to a health care institution.
b) the patient is transported and transferred to another institution (see paragraph access to the health care institution).

Detection of narcotics, weapons and ammunition:
If during diagnostic examination or medical treatment in or at the body of a patient narcotics, weapons or ammunition is found, the knowledge becomes subject to professional secrecy. It is recommended - taking the safety of staff and other patients into account - the follow the following policy:

- The narcotics, weapons or ammunition (also found in the body) will be handed over to the liaison officer or designated officer, which will hand it as soon as possible over to the police. The origin of the drugs, weapons or ammunition will not be disclosed to police. To guarantee the safety of health care employees the police will collect the narcotics, weapons and ammunition at the hospital.
- The police issue a receipt to the person who deposits the narcotics, weapons or ammunition on behalf of the health care institution. On request the patient receives a copy of the receipt.
- The patient is informed at which police station the narcotics, weapons or ammunition has been deposited. If the patient believes a claim can be made, he or she can report him/herself at the police station.

Access to the health care institution:
The main rule is that investigating officers (police) may freely enter spaces that are open to the public, such as a lobby, waiting room or hallway. A planned visit by the police should be announced in advance. Unscheduled visits need to be reported to the security department and /or the liaison officer as soon as possible. Any space occupied by a hospitalized patient is considered a house. Entering without consent is breaking a constitutional right. Areas that are being used to provide medical treatment (e.g. ambulance, treatment rooms, consulting rooms and operating rooms) are not covered by the constitutional rights, but are in principle not open to police officers based on the obligation of the hospital and its employees to carry out treatment without been observed by others. There is only one exception made to this rule; if both admitted patients as the Board of Directors provide consent to enter. This arrangement runs via the liaison officer. Exceptions to this rule are possible, which are discussed later in this paragraph. The police should always (even when entering non-private spaces) first identify themselves and communicate the reason for their arrival (rescue or detection) and on which grounds they like to enter. Although the police officer dressed in uniform is not legally obliged to identify itself, it is still desired (a uniform does not provide sufficient security to the institution to actually establish dealing with police). Resulting from the covenant identification and explanation by police runs via the liaison officer (or a designated liaison officer). All contacts with the medical staff are run via the health care institution's liaison officer. An arrest can be made anywhere a suspicion of an offense exists, even without the consent of the patient and/or his physician. When an arrest is made the police will, if possible, first contact the liaison officer and via the liaison officer with the medical staff involved in the treatment. When there is a medical objection to the transfer the patient, police will be informed via the health care institution liaison officer. When a part of the institution is considered a *home*, the provisions of the General Law to enter are applicable. In many cases the institution will observe the house right of the patient to third parties: where a patient spends its private life (this can be a section of the institution, think of a room where he/she stays), can be considered to be a dwelling. Entering a dwelling which is indicated as a *home*, without the consent of the patient, with the aim to arrest the patient as a suspect, is possible under the following circumstances:

- by the police officer with a warrant to enter. Exception is the case to enter immediately to prevent serious and immediate threat to the safety of persons or goods.
- by the Public Prosecutor himself (without a warrant to enter).

Entering areas with hospitalized patients should be done with caution and pre sought medical advice. The principles of proportionality and subsidiarity are applicable and the harm to the health of the patient, who is considered a suspect, and other patients sharing the same space should be minimized as much as possible. When a patient is put into custody he or she shall be guided within three days and fifteen hours to the magistrate. The magistrate will assess whether the arrest and detention is lawful and will therefore always hear the suspect. The counselor of the accused will be present. When the accused at the time of arraignment is admitted in the hospital and for medical reasons should remain, the Magistrate, accompanied by a clerk, will hear the suspect in hospital. The Magistrate consults the hospital's liaison officer prior to the arraignment. Medical staff needs to be aware that the lawfully entering of a care area by an officer of police or Public Prosecution does not prevent the employee to remain bound by professional secrecy. An acute emergency is an exception to this rule.

Guarding patients:
Reasons to guard patients may include: protection of the patient because it is feared that he/she can become a victim of a crime (again), protection of other patients and/or staff, or to prevent the patient that has been detained by the police to flee. Patients deprived of their liberty by law, but should undergo medical treatment, are guarded by the police. It may be patients that are arrested before their arrival in the institution - in that case the patient will enter the health care institution under supervision - or patients who have been detained in the institution and cannot be transported. In principle, the patient that has been deprived of their liberty stays (in consultation with the liaison officer) under supervision of the police. The supervision by police is also to protect the employees. Once treatment allows the patient, who is deprived of his liberty, to be transported, he/she will be transported to a police station, penitentiary hospital or correctional institution. On the method of guarding the police consult the health care institution's liaison officer. The police inform the liaison officer as soon as the patient supervision is terminated.

Seizure of properties of patients and of the hospital:
If it is not imperative to seize goods directly, the goods will be seized after a written request in retrospect. In case of *flagrante delicto* of an offense or in case of suspicion of a crime for which pre-trial detention is permitted, the investigating officer is authorized to seize objects susceptible to seizure and for that purpose enter any premises. Investigators may freely enter areas intended for the public, such as a lobby, waiting room or a corridor. Patients admitted to hospital and stay in a patient room can invoke on their constitutional right house right. This constitutional right means that investigators can only enter areas as wards and patient rooms with the consent of the patient or with an authorization of the Public Prosecutor to enter a dwelling (hospital). A doctor or hospital is required to provide access to an authorized police officer. This does not relieve the police (and Public Prosecution) from their obligation to consult with the physician before the investigating officer proceeds with official acts. This consultation relates to the medical condition of the patient. If a search of a patient room or ward is required, the investigating officer needs to be accompanied by a Magistrate and a Public Prosecutor or a Deputy Public Prosecutor. In

case of urgent necessity and if the action of the Magistrate cannot be awaited, the Public Prosecutor or Deputy Public Prosecutor can search a patient room or ward without a Magistrate, provided they have an authorization of the Magistrate. Susceptible to seizure include goods obtained by crime, which are important for identification (e.g. clothing from the patient), goods which has been used to commit an offense (e.g. weapons) or that are important for truth finding. The police should provide as much documentary evidence to the person, under whom the goods were seized, indicating which goods were seized. Seizure of letters and other writings which fall under the professional duty of confidentiality, such as records, prescriptions and patient administration of subjects with privilege, e.g. doctors, by investigators are in principle prohibited. On the prohibition of seizure is an important exception: a copy of the file may be seized if the doctor agrees. This is possible with the patient's consent and/or if there is a conflict of duties. When a conflict of duties occurs only in very exceptional circumstances the importance of truth can prevail. These include very serious offenses such as murder, rape and/or very sensitive social issues. If the doctor himself is a suspect the preceding rule does not applies in relation to confiscation of the medical record. In that case, the institution's liaison officer contacts the Public Prosecutor.

Blood Tests due to driving under the influence and DNA Testing:
If blood samples have to be taken by patients in a health care institution due to driving under influence, the police will make use of a licensed forensic doctor. For the forensic task of taking blood samples special doctors are designated per region. The forensic doctor will contact the hospital's liaison officer, unless otherwise agreed, to carry out his/her task. The forensic doctor assesses, possibly in consultation with the attending doctor, if blood sampling is medically justifiable. If treatment is necessary in the Emergency Room this has emergency has priority over the taking of blood. For a blood test the consent of the patient is required. The forensic doctor asks for the consent of the patient's blood. When the patient refuses, the Deputy Public Prosecutor can order him to cooperate with the blood test. When the Deputy Public Prosecutor is not available, other investigators / police officers may also give this command. If the patient still refuses after this command, although this yields an offense, this does not mean that the patient must participate in the blood test. He cannot be forced to do so. If the suspected patient is unconscious, his blood may be taken indeed, but the blood test cannot be held before the patient has given permission. In the event authorization is not obtained, the obtained blood will be destroyed.

Removal of cellular material:
By the removal of cellular material of a suspect is meant the collection of fingerprints, material from under fingernails, and gun powder traces on the body. In the situation of *in flagrante* the police are allowed to secure such traces. It is - if the patient is conscious – required to have the patient's cooperation. The Public Prosecutor can command in the interest of the investigation to take cellular material from the patient who is suspected of a crime on which detention is authorized and charged with a serious suspicion. The Public Prosecutor gives the command only after the patient has been interrogated. The patient is authorized to be assisted by a counselor during this interrogation. For the removal of cellular material for DNA testing the consent of the patient is not required. When incapacitated, DNA material only can be taken after an order of the Public Prosecutor.

No conviction of natural death:
Each municipality has a number of forensic doctors appointed as municipal coroner. If there is no certainty about a natural death:

- the practitioner informs the coroner without delay.
- the ambulance care worker or the police informs the coroner.

The current situation should be preserved in its original state if possible. The forensic doctor will inform the Public Prosecutor of his findings. The Public Prosecutor decides on the further procedure. If a declaration of natural death is already issued, but in this regard during the autopsy in hospital doubt occurs, the autopsy is immediately discontinued and the forensic doctor will be contacted immediately. The forensic doctor will inform the Public Prosecutor of his findings. The Public Prosecutor decides on the further procedure.

Sexual offenses:
In case of sexual violence the victim decides if he/she will file a report at the police. When a sexual offense is reported, an intake or a police report can follow. The crime scene investigation is basically conducted by the forensic doctor. In special cases, e.g. upon request, the physician may do this in the presence of the forensic doctor. If a victim of a sexual offense is unconscious, the crime scene investigation can still be carried out. The submission of the content of the research is not send until the victim provides consent. The results from the research can also be investigated without providing the name of the victim.

Child Abuse:
When child abuse is suspected the employee of the health care institution will contact the Advice and Child Protection Agency according to National Reporting Code. The Advice and Child Protection Agency will decide to report the child abuse to the police.

Aggression and violence against employees:
The following definition of aggression and violence is used by the program Safe Public Task: "The verbal expression, the use of physical force or power, or the threat to use force, against an employee, under the circumstances directly related to the execution of the public task, which results or would probably result in a feeling of threat, property damage, injury, mental harm or death." From 'good employer perspective' due diligence is an obligation of the employer to ensure a safe working environment. Every covenant partner gives high priority to battle aggression and workplace violence incidents. The health care institutions shall ensure the coordination of all matters that can contribute to achieve the objectives mentioned above. Each covenant partner takes care for a protocol managing incidents of aggression / rules of conduct Safe Care / code of conduct / safety protocol against aggression and informs each employee of the contents of these protocols. The police liaison officers and the Public Prosecution receive copies of these protocols. The 'protocol' contains at least the following components:

- Determine forms of aggression and workplace violence
- Set a standard of acceptable behavior and make them known to outsiders (clients, patients, visitors, etc.)
- Preventive measures
- What to do in an acute situation
- Repressive measures
- Discontinuation of service
- What to do when providing aftercare
- Reporting and willingness to report
- Policies relating to the recovery of damages
- Important telephone numbers

- Registration of incidents, reports and declarations

The employee or health care institution will contact the police by making a notification or declaration according to the aggression protocol of the institution. The employer has the responsibility to determine when notification or declaration is made, apart from the right of the victim to do it him/herself. The employer can indicate the employee for instance with a Number when filling a report. The employer can make a report on the basis of the Code of Criminal Procedure. This states that a person, who has knowledge of an offense, is competent to file charges. The victim will, if necessary, be heard as a witness/victim. The victim of aggression and workplace violence can provide the address of his employer rather than its own address when filling a report. The police must provide the employee the opportunity to use the employers address in cases of executing the Safe Public Tasks, regardless of the nature and seriousness of the offense. Furthermore, it is possible in certain cases to file a report 'under number' where the criteria are tested by the Assistant Public Prosecutor. This procedure must be separated from the anonymous declaration. The latter is a separate procedure that only in very exceptional cases is followed. If the declarant wishes the police can make a 'deployment request' (appointment on location) in their information system. This is an entry in the police's information system in the district or residence of the declarant, so it can react more alert on a request for assistance by the declarant. This is supported by Public Prosecution. Such a request may also be filed through the security department of a health care institution. When filling a report it must made known that it handles the execution of a public function. With the police and Public Prosecution agreements are made on the handling of aggression and workplace violence against officers with a public task. For example a high priority is given to the investigation and prosecution of perpetrators. Also higher penalties are demanded. These agreements are defined in the Uniform National Agreements. The police and prosecution will do everything in their power to make reporting as easy as possible and process the declaration as soon as possible. The threatened or abused employee should be aware that for a proper handling of the filled report an accurate method is required. Police and/or Public Prosecution keeps the declarant/victim informed on the settlement within the framework of the law. Each institution promotes the willingness to report and record incidents of aggression incidents, reports and declarations, formulates a policy in which situations the institution at least files a report and facilitates employees to file a report. Every covenant partner indicates someone responsible for registering all incidents / reports / declarations centrally as well as the course of the procedure. Police and institution conduct a proper registration on all incidents of aggression committed in and under the direct control of the health care institution. ☒
The police liaison officers and the health care institution's liaison officer at the local level will at least meet 2 times per year to hold consultations on the preventive and repressive actions taken. If necessary, others are invited. The police contact officers, Public Prosecution and the health care institution shall provide a joint annual report.

Employee who is regarded as a suspect:
If an employee is suspected of committing (or involved in) an offense or crime in his or her profession, the police contact the health care institution liaison officer. The role of the Board and the liaison officer will vary by institution and by each situation. An employee can arrest anyone for a crime when caught in the act. The suspect must be handed over to the police as soon as possible. An employee can be arrested by the police after the criminal act has been committed, but only after consultation with a Public Prosecutor. After his/her arrest, the employee will be brought before a Deputy Public Prosecutor. After arraignment of

employee he will be interrogated by police. He cannot escape interrogation but is not obliged to answer questions. Prior to the interrogation, the arrested employee may assisted by a counselor. If the employee is not detained, the police can ask him to come to the police station for questioning. The police initially have six hours to complete the criminal investigation after arrest. However when an offense or crime is committed, which is admitted to remand, the arrested suspect can be detained longer (up to 3 days) in the interest of the investigation ordered by the (Deputy) Public Prosecutor. He/she will then be detained by the Public Prosecutor. When the Public Prosecutor becomes aware of an offense he/she can claim a preliminary inquiry by the Magistrate. In this phase, suspects, witnesses, and experts can be heard and certain coercive measures such as search and seizure can be applied.

Partnership reviewed:
Since 1998 the covenant has contributed in creating a mutual understanding between police, Public Prosecution and the health care institutions, which results today in a workable relationship. Furthermore, the covenant has been become more popular among health care institutions which resulted in increased participation and a strong urge to make the covenant sustainable for the coming future.

Publications Committee/Newsletter Editor: **Mr. Robert E. Lee, Jr.; Lee_Robert@Cox.net**
Assistant Editor: **Mr. Ray Ferrara, CPP; Ray.Ferrara@Ferguson.com**