Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4 (Amended April 8, 2002)

Norman Witt

Ethics in Your Day, Your Job and Your Next Decision

> A man's ethical behavior should be based effectually on sympathy, education, and social ties; No religious basis is necessary. Man would indeed be in a poor way if he had to be restrained by fear of punishment and hope of reward after death.
> --Albert Einstein

The ethical issues that network and systems security professionals must face each day have changed dramatically since that Tuesday of September 11, 2001. On the job, on a day-to-day basis, most IT workers would probably view the essence of ethics as knowing the difference between right and wrong and being able to choose between them, and struggling through the gray areas in between. But what and where are the rules for doing this?

This paper will attempt to describe what ethics are and do in our daily lives. Much of the current writing on IT ethics views it from a safe, 10,000-foot altitude. Finding any writings that deal directly with the day-to-day, hour-to-hour challenges the IT security worker will face is less productive. It seems the assumption is that we will know the correct ethical and legal direction and choose it as any other person would. But really what guidance do we have? Will our own sense of ethical behavior and what the law dictates always coincide? What would a good code of ethics include? What makes a code work in the daily grind of what is commonly the over-stressed, over-worked job of IT security? Can a code of ethics relate to a ponderously legalistic tome such as the Health Insurance Portability and Accountability Act (HIPAA)? This paper shall attempt to address those issues.

Defining Everyday Ethics

The Merriam Webster Collegiate Dictionary defines ethics as:

a : a set of moral principles or values **b :** a theory or system of moral values <the present-day materialistic *ethic*>,,, **c** *,,,* **:** the principles of conduct governing an individual or a group <professional *ethics*> **d :** a guiding philosophy [1]

Everyday ethics can be described as how you relate to your community every day. In our case the "community" is our co-workers and our work environment. Ethics are a function of community. At their roots, communities of people are based on common sets of rules, behaviors and values that a group of individuals are willing to share. Individuals are willing to share these common beliefs because they see them as to their own benefit and profit. The community offers strength and security to its members; it is greater than any individual in it.

Thus far, no community has ever existed where all of the included individuals shared all values and beliefs absolutely. Individuals will disagree with some aspects of, and events within the community. But so long as the members of the community feel that they can agree upon a basic set of values and beliefs, and recognize that the community depends upon these beliefs and values to remain relatively stable, each community member will remain and abide within the community and accept the differences about him. In return, the individual is expected to contribute to the maintenance and governance of the community. You could call this the Social Contract. Thus, the community is the manifestation of a common ethic.

Your personal community probably is the group of people you work with everyday, your family, and your neighbors. That community is part of the larger communities of the city, the county, the state, the nation you live in. For our purposes these political entities will serve as social community units. They provide a common identity for individuals to share – we are New Yorkers, we are all Americans. All will share a common root set of values, beliefs and behaviors that the individuals recognize as shared by all, though these values and beliefs will become more generalized and ambiguous the higher you go in the meta-structure of communities. Members of the community that violate the common ethic have offended against the community and perhaps have violated a law since laws are to some degree the codification of the common ethics.

This is, of course, a vast simplification of the human social dynamic, but you should get the point. A person who violates "his" or "our" ethics has offended individuals in the community and, thus, the whole community. He has not kept the conditions of his social contract.

This is certainly not intended as a political or as any kind of religious statement and nobody should view it as such. It is simply an attempt to describe how your "everyday" fits into larger schemes. This helps form the basis of what you may view as your personal set of "ethics".

Legal and Ethical Dilemmas

Pimm Fox reported in a ComputerWorld article a year ago that South Carolina had passed a law stating that you as a security professional in South Carolina might be

required to monitor your fellow employees to see who is looking at child pornography on his or her computer, and "IT pros who see child porn on an employee's computer must report the name and address of the owner or user." Not reporting it could make you an accessory to any crime that co-worker might be charged with later [(2)].

What if you report somebody and you are mistaken? How many IT people would be familiar enough with the law to know exactly what is legal and what is not? Anybody who thinks they will not be affected by legalities in their job is not paying attention. Most employees are at least acquainted with their employer's policy of permissible computer use on the computers provided by their employer. But when you see an article or paper that discusses the legal aspects of security, what is it that you usually see in the opening paragraph – the disclaimer that the information provided is by no means to be taken as legal or authoritative advice and you should see an attorney for your particular issue (and to be told the same advice). So what ever they are afraid of I want nothing to do with, either.

Mr. Fox's article indicates that you must report this suspected crime to legal authorities, with no mention of informing your employer. What rights would the employer have in the glare of publicity that such an offense would attract? What are the employer's legal options?

Mr. Fox states his feelings against such laws in language most would probably agree with:

> IT workers shouldn't have to police other people's computers. They aren't trained to enforce the law, they don't have insurance protection if they make mistakes, and they won't appreciate being the thought police. (Fox, page 1)

However, he goes on with a statement that I wonder how many would endorse as enthusiastically;

> IT workers shouldn't be held responsible for other people's illegal behavior. Imagine being prosecuted as an accessory because you knew about child porn on a computer but didn't want to be a rat. (Fox, page 1)

Here we find a clear conflict in personal ethics. Why would you NOT report a crime like child pornography to the proper authorities, whether you are in South Carolina or not? Perhaps the South Carolina law does go too far in requiring IT workers to report *suspicious activities* among their neighbors. However, does your personal ethic provide that it is an individual's right to engage in what most of the community would consider a predacious vice that is satisfied by activities cruelly exploitive of the most vulnerable members of society? Sorry. It's get-to-know-your-cellmate time.

Very few of us will be faced with such daunting choices. In fact, our challenges shall be more mundane. However, the challenges on the job will be enough for most when you consider the sources of conflict for your personal ethics can come from within as well as from outside.

By many accounts, the Cybersecurity Plan being put together in Washington is being rendered ineffectual by the pressure of high-tech industry lobbying. The reasons for this are, of course financial. A Washington Post article by Brian Krebs on September 19, 2002, describes the industry's reluctance to go along with anything that means taking responsibility and the current administration's willingness to cater to the industry's wishes [(3)]. Any liability or responsibility laid on the industry by the cybersecurity initiative could mean huge costs in the uncertain economics of the day.

Many of the initiative's recommendations are aimed at improving communication between government and the high-tech industry to better enable a coordinated and informed response to a threat to the technological infrastructure. However, many companies are still reluctant to share any information they might have about security vulnerabilities, intrusions, or flaws in their products. Their concern is their legal liability, or even the suggestion of it if they were to be sued by a customer or shareholders. In Krebs' report, the dilemma that corporate executives could find themselves in puts any ethical choices they might have had in perspective. He quotes Bruce Schneier, chief technology officer and co-founder of Counterpane Internet Security,

> You really have to ask why CEOs would bother to follow any of these recommendations, particularly at a time when most companies' earnings are down 20 percent. ,,, The fact is, companies aren't rewarded for altruism; they're rewarded by the strength of their stock price.
> (Krebs, page1)

Most corporate executives, at least from the somewhat jaundiced point of view of some of their employees, are not going to be caught in the grind between any altruistic feelings and their corporate responsibility to look after the bottom line. And when the bottom line is what is guiding company management, how do you think that is that going to affect the corporate ethic at those lowly points where the income is being generated?

The Guy on the Spot Supporting That "Bottom Line"

How do the people working in the trenches perceive themselves as ethical decision-makers? Much of that may depend on how they perceive their leadership and their organization. Common stereotypes are easily created. In a April 3, 2000

ComputerWorld article by Paul A. Strassmann, he reported finding this announcement;

> A forthcoming conference for IT leaders features a tutorial that includes as topics "how to make other people cringe and whimper when you enter the room," "how to get what you want when you want it whether you deserve it or not," "how to act . . . without morality," "how to leave kindness and decency behind" and "how to seize the future by the throat and make it cough up money." The entire conference is offered to IT executives for a fee of $2,380 each and to consultants for $10,000 each, with an additional opportunity to purchase a book that includes lessons on "how to get mean and nasty" and how to "lie when necessary [4]. (Strassman, page 1)

And how about the personal ethics of those lowly professionals who are in the positions where they can push the ethical envelope when it comes to corporate security of data and personal and proprietary information? A ComputerWorld article by Mitch Betts on May 22, 2002, called “Dirty rotten scoundrels?” tells quite a tale about us [5].

ComputerWorld took an ethics survey among IT professionals and found that while most say they would pay the registration fees for shareware, 47 percent also said that they had illegally copied commercial software. Smaller numbers of us (15%) can see the hackers’ side of things and fewer yet will admit that they have looked in confidential files. On the plus side most say they would not discuss confidential information about celebrity customers they happen across. The ComputerWorld survey also found that 73% say they would “blow the whistle if their company planned to use information systems in unethical ways.” That may be fine to say in a survey but the reality may be something else, since the “actual deed is hard to do because society treats whistle-blowers like schoolyard tattletales, and some whistle-blowers end up transferred, demoted or fired.” (Betts, page 1)

It would seem that ethics are held in high regard but that many of us may feel we are not up to the standard required, or that while ethics are important they can get in the way of a good thing. However, Mr. Betts goes on, saying that when there has been a breakdown in ethical behavior, the usual corporate response is to write or re-emphasize the company code of ethics. How much good this does is open to debate.

There are probably many companies and organizations where the annual ethics “training” is more a humor break for the employees and provides them an excuse to speculate about how much attention the execs that decreed the training personally pay to the ethics standards they would have their employees “learn” in these sessions.

Winn Schwartau writing for Network World reports that when running one of the many "Cyber Ethical Survivor games" he has done, he asked the usual question of two teams; if you suddenly had the details of a business competitor's project fall into your hands, and it's enough for you to beat them out if you used it, would you use it? In this one instance he found one team said that they would use it, rationalizing it with the "Business is war" credo. The other team disagreed completely, taking the opposite position that to use it would be unethical and maybe illegal. It would be "cheating" to win like that [(6)].

Mr. Schwartau was impressed with two things;

> First, that the two teams were so diametrically opposed; and second, that there was almost no dissent among the members of each team, even though the players had been randomly selected from a large audience and didn't know one another. (Schwartau, page 1)

This experience was contrary to Mr. Schwartau's usual results in these seminars in the United States and in European countries. He usually sees both teams and the audiences at these sessions leaning one way or the other with apparently no prevailing tendency to chose one side or the other. His conclusion from this experience is, "there is no cyber ethical consistency across the spectrum of computer users, security professionals, consultants, executives, military leaders and technical staff". (Schwartau, page 1)

You might also conclude from this that ethical considerations can be guided by the herd mentality; that those more aggressive types who speak up first will set the tone and direction of the other participants. This creates an interesting dichotomy in that I believe the real day-to-day (and albeit, smaller) ethical challenges for IT security types come at times when you are essentially alone in the process, when you are the one making the decision and you are not likely to be seeking consensus among your peers. What will either help or hinder your decision processes are what you personally believe, what you have learned about your employer's ethics policies, and whether the principles of that ethics policy are a real part of the environment or just a list of rules with little to do with your everyday job.

Finally, Mr. Schwartau gets into what we are really after here. The point is we should not have to dwell on questions and uncertainties about ethics issues, but "Cyber ethics" should be as much a part of our day and as normal as access lists, any/any/deny, or intrusion events. He defines the following points;

- There must be formal policy guidance. ",,, that boring set of guidelines and rules that human resources gives every employee. Most security-aware companies provide staff with a reasonable set of black-and-white policies: Do this; don't do this". (Schwartau, page 1)

- And before an organizational culture can make a policy a working ethic, add the following;
    - "Cyber ethics is a leadership issue". (Schwartau, page 1) As he found in his seminars, one leader will emerge and set the standard for the whole group. It is necessarily a management function but is on those individuals who will speak up and have a clear image of what their ethic is. They can influence and move others by their words and example, for better or for worse.

    - This leadership is not about management or designated individuals. It is about the organizational "culture" they live and work in. Those that fall into this leadership role may be better able to articulate that cultural ethos (modified by self-interest, of course) for those whose feelings are more ambiguous.

- There should be "cyber ethical components" (Schwartau, page 1) included in any corporate attempts to foster security awareness among employees.

- These policies should be adaptable and upgraded as circumstances may deem necessary. This not to say we are setting up situational ethics that can change at your convenience or to maximize your benefit. The September 11, 2001 events brought many ethical considerations to the fore that we had not really had to directly face before. Whatever may happen tomorrow may have a similar effect.

To help develop a clearer concept of ethical thinking generally acceptable to the IT community, we should define our broader responsibilities. We are all "fiduciaries" with "fiduciary" responsibilities, whatever that is, and we will examine codes of ethics that are already out there in the IT world that may give us a better definition of what our greater responsibilities may be.

Fiduciary Are Us

How many of us have stopped to consider ourselves as "fiduciary", or even what fiduciary means? Defining "fiduciary" may put defining parentheses around our job and our profession, and help clarify our ethical/legal responsibilities. But it is one of those things that can be rather daunting in its legal and ethical implications. At least we know where we stand. The glass is half empty.

Malcolm Lloyd wrote a paper on the fiduciary responsibilities of organizations, executives, and managers as the Comprehensive of his doctorial degree through Capella University [(7)]. In this paper, he defines "fiduciary" thus;

> A dictionary definition of fiduciary is "trust, a thing held in trust. (McKechnie 1979.)" A legal definition of fiduciary is " In general, *a person is a fiduciary*

> *when he occupies a position of confidence in relationship to another person or his property* (Robert & Corley, 1967.)" *This position of trust extends to organizations and, in particular, the people who carryout the functions and policies of those organizations*.,,, this fiduciary understanding includes things in electronic form and relationships carried out in electronic communications. ,,, fiduciary responsibilities exist for an organization's employees, staff; customers, business partners, competitors, clients; stockholders, management boards, the public, and governmental agencies. (Lloyd, page 3)

I italicized those portions of the definition above that are key to us as IT professionals. It is accepted that we do hold a position of trust in our jobs. Anybody who has traced /sniffed on a network figures that out quickly enough. Yet how many of us are formally bonded or insured for our professional responsibility and the "position of confidence" and trust that we occupy? Were you instructed in the finer points of confidentiality and company proprietary information before you read your first network sniff? Most often in the past it has been the implicit understanding that we were aware of the responsibility we took on with the job. Can we afford that anymore?

Mr. Lloyd cites several studies in his paper and their findings that,

- Ethical perception and decision differences,,, could be associated with generation, education, cultural, group attributes, or task orientation.

- There are differences between IT professionals and students and that those in the studies tended to "oversimplify ethical issues" or failed to consider all factors that might be at work in ethical issues, such as their own alternatives, others involved in the issue, or their own duties – their "fiduciary responsibilities".

- A study by Boomer et al (1991) found ethical reasoning differed among those studied by age, education, and years in a profession. (Lloyd, pages 4 - 5)

Mr. Lloyd cites another study that researched "the effects of organizational policies and climates or cultures on "situational ethics" and found that such ethical decisions can be favorably affected when executives and managers establish ethical climates in their organizations". (Lloyd, page 5)

Fiduciary responsibility could be seen as providing a layer of legal and organizational definitions over the more ambiguous societal forms of ethical understandings, and thereby providing much more definitive context for the job and for organizations. A code of ethics can be better understood when it can be explained in the context of your job and your work environment. Fiduciary responsibility adds levels of legal and fiscal obligation that might not be present

otherwise. Fiduciary responsibilities extend to your employer, customers, and your fellow employees. For company executives, they extend to shareholders and to the community in which the company resides.

Mr. Lloyd explains that from legal and social viewpoints, fiduciary responsibility is seen as residing with the organization "through its officers, managers, and information technology administrators". (Lloyd, page 12) While executives and officers of the organization bear the brunt of this responsibility, each "agent" of the organization can be held accountable to a lesser degree for fiduciary responsibility within his area of involvement.

Violations of fiduciary responsibility can be sins of omission or of commission. At the heart of this responsibility is the legal principle that ignorance is no excuse. Not knowing the law, or ignorance of vulnerabilities or flaws in products, processes, or your implementations does not excuse you or the company of responsibility.

The Federal Sentencing guidelines provide factors that are used to score degrees of culpability of senior executives in their organization's failure to uphold their fiduciary responsibility, and conversely, can be used to measure an organization's effectiveness in upholding their fiduciary duties.

Mr. Lloyd writes in his conclusion that organizations assume a wide and constantly changing array of fiduciary responsibilities when they use networked information systems.

> Not knowing of these responsibilities is, in itself, a failure to perform in a fiduciary manner and results in vulnerability. ,,, An organization is required to have information policies, communicate them to their members, stipulate disciplinary actions when policies are violated, and continually review, update, and revise polices and information systems to maintain fiduciary responsibilities. (Lloyd, page 13)

As Winn Schwartau had found, Mr. Lloyd concludes that the culture of the organization will influence the members in their behavior, so if the business culture is conducive to ethical decision-making, the members of that organization will tend to make decisions based more solidly on ethical considerations. And so, "executives and managers need to understand and establish a principled ethical climate where by institutional members will decide most ethically regardless of their locus of decision" (Lloyd, page 16), and this will foster and promote the process of ethical decision-making and upholding their fiduciary responsibilities within their organization.

Codes of Ethics: Beginnings

So what is a code of ethics that fits your every day? It is probably something you are not going to think much about until some ethical issue is in your face. The best code is one you aren't thinking about until you are faced with the choice that brings it to mind. It may be that such ethics awareness will arise from the workaday emphasis that the "culture" you work in places on ethical decision processes.

I heard a story recently about a company with a facility that included a couple hundred developers and programmers. Some security types cruised through the building with a laptop with a wireless modem to see how many wireless AP's they might find. They found four, 2 of which were wide open to the company network. In this stroll they casually spoke about the security concern to 3 people. No official management of interest was contacted. A week later, no wireless AP's were found. It seems the company policy about wireless AP's on the premises was not well known or undeveloped. But once the security issues were communicated, even in a casual manner, the AP's were shutdown voluntarily until a more secure configuration could be set up. This may be unusual, but it does show that among a broader spectrum of IT people they are at least aware of the self-interest in what is good for the company is good for them. And perhaps it was more than that, too.

Winn Schwartau in his Network World article of July 2, 2001, "Needed: An Electronic Bill of Rights", was irritated by what he saw as the watering down of meaningful legislation to protect everybody's online rights [(8)]. Mr. Schwartau proposed a six-point "Electronic Bill of Rights" that he felt should provide the basis for any future online rights legislation. His bill of rights included;

1. I own my name. It is mine to do with as I please - not yours.
2. You, as a business, may use my name for the purpose of our transaction only. You may not sell, barter or otherwise market my name, or any information about me, without my explicit permission.
3. If you need to keep my name in files for the purpose of ongoing business, you will protect it from abuse, illicit access or accidental release.
4. If you have any files containing my name, you must notify me of the existence of those files, send me copies on request and provide a reasonable means to add, delete or correct information.
5. The government will create a new data classification called "Personal but unclassified," and set standards for its protection in the private sector and for legitimate government needs.
6. I will have civil and criminal recourse against persons and organizations, private and governmental, that violate my Electronic Rights or let them be violated. (Schwartau, page 1)

Mitch Betts in his "Dirty rotten scoundrels?" article points out that a code of ethics is no answer in itself [(5)]. He says that even more important could be an organizational culture,

,,,in which employees feel free to admit mistakes, air bad news and raise ethical concerns without fear of hurting their careers, ,,, Otherwise, project status meetings are full of happy talk and no one raises the critical issues." ,,, "Ultimately, the IS department's approach to ethics will be determined by the corporate culture, the moral fiber of the IS employees and the priorities of the top IS executive. (Betts, page 1)

Mr. Betts then proposes a 10-point ethics checklist of questions for CIO's that should help them create the culture of confidence in their workplace. Those questions are;

- Can employees report project delays and problems without fear?
- Do we have licenses to cover all software use?
- Do we have enough independent auditors to root out computer abuses?
- Do we have an ethics code that is well publicized, updated and enforced?
- Is there a clear, enforced policy on data confidentiality?
- Is there a policy on monitoring employees' electronic mail?
- Is there a policy on proper use of on-line services and the Internet?
- Is our ethics code based on real situations?
- Are social/ethical implications discussed at the start of system projects?
- Do we explain the biases and limitations of our systems to users?
- Testing to weed out the liars
  (Betts, page 2)

A good code may not be known by its verbiage but the idea and general principles should always be implicitly understood in the work environment. I think the story about the unguarded WAP's indicates, in general, that IT workers would be predisposed to cooperate and work within the rules IF those rules are known. They would do this for their own self-interest if for no other reason. And perhaps more altruistic reasons would also arise.

If one is unclear about any code that their employer has published, or if there is no specific code, Winn Schwartau's Electronic Bill of Rights and Mitch Betts' ethics checklist should provide context, a point from which you can begin to understand what the a code of conduct should address.

Codes of Ethics: Prime Examples

A Google search on "code of ethics" "Internet" "Security" will return over 25,000 entries. It is easy to find any number of good codes of ethics, but I have singled out two that should provide good reference points.

The Computer Ethics Institute of the Brookings Institution in Washington, D.C., has provided "The Ten Commandments of Computer Ethics" in an effort to foster

better online behavior and proper use of the technology [9]. Among their ten "Thou Shalt Not's" there are tenants about not harming other people, respecting others' privacy, respecting copywrites and intellectual property of others, and showing respect and courtesy online. It has the virtue of being simple and easily understood, and is general enough that you can read it and retain its principles.

The "ACM Code of Ethics and Professional Conduct" in the bylaws of the Association of Computing Machinery is more formal and structured, containing bullet items under the headings "Moral Imperatives", "Professional Responsibilities", "Leadership Imperatives" and an ACM members' vow of compliance with the code [10].

As they say in the Preamble to the ACM code, it consists of 24 "imperatives" of responsibility and commitment on the part of their members. They have attempted to address many of the issues that IT professionals may face. The ACM has provided a set of guidelines that are meant to clarify the imperatives and responsibilities in their code, and to make it more applicable to the daily events that will arise in their members' professions.

This is indeed, a professional's document. It is serious in content and in the commitment they require of their members. A more cynical view might think their language and pronouncements to be on the righteous side of the Boy Scout Oath. However, it really comes down to what kind of professional do you consider yourself to be?

Professionalism means you hold yourself to a higher standard because you are good at your job, you believe in it, and you believe there is a minimum standard of knowledge and performance that you must maintain to remain a professional doing a competent job. Failure in this becomes unacceptable.

The ACM's imperatives require the membership to "contribute to society and human well-being" as their first commitment. To "avoid harm to others", to "be honest and trustworthy", to "Be fair and take action not to discriminate" are at the top of their list of moral imperatives. (ACM, page 1) Their guidelines add to the details of each imperative and try to describe circumstances that could apply.

These and the rest of the code read as pretty high-minded stuff, but in these uncertain days of questions about ethics and responsibility, perhaps it is time to take a queue from such idealistic statements. It isn't just a job. It isn't just a paycheck. No matter how downtrodden you may see yourself as an employee, there is a seriousness to your duties that was not there before. It would be well to have some guidance to help navigate the rules under which we now must operate.

A Code Fit for a HIPAA

The Internet Healthcare Coalition sponsored the eHealth Ethics Initiative and in May of 2001, they introduced their International Code of Ethics. This became known as the eHealth Code of Ethics. Bette-Jane Crigger of the Hastings Center presented a paper titled, "Foundations of the eHealth Code of Ethics" at the 2001 Quality Healthcare Information on the Net conference [(11)]. The premise was that the IHC believes that Healthcare over the Internet has a vast potential to improve human well-being by providing global access to health information and related commercial resources. Fundamental to their eHealth Code was the need to foster trust, which they consider the biggest obstacle to developing online healthcare. People on both sides of a internet communication about healthcare must believe that the person on the other end is whom they say they are, that the information they exchange is relevant and accurate, and that that information is going to be kept confidential.

The genesis for the eHealth Code was to begin the process of building this trust among healthcare providers, patients, site sponsors and others involved in any online healthcare transaction.

The principles of the eHealth Code of Ethics are be summed up in just a few words, as they are in the document itself; "Candor", "Honesty", "Quality", "Informed Consent", "Privacy", "Professionalism", "Responsible Partnering", and "Accountability" [(12)].

Candor means that when people use healthcare sites on the Internet they should be able to see who has a vested interest in the site, what purpose the site is to serve, and any commercial interests that might be involved behind the web site.

Honesty means that people should be assured that any claims or information at a web site is not exaggerated or misleading. All advertising should be easily identified as such and not easily confused with educational or informational content.

Quality should be in the information and data on these web sites. These site providers must evaluate information presented for accuracy, that it is current and best available, that those that provide the information are fully qualified and competent; indicate the sources of information, and present all sides where there may be multiple points of view.

When people are to provide personal information on the Internet they have the right to Informed Consent. That is, they must be informed prior to providing the information how it will be used, the potential risks involved in providing the information, who is collecting the data, who will see the data, and how the data will be used. Data should not be collected, used or shared without the user's "affirmative Consent". (IHC, page 5)

All users of these web sites have the right to expect that the information that they provide will remain confidential. They should be able to expect their Privacy will be respected and maintained. The site should provide preventive measures from unauthorized access, trace how the data is used, and render data unidentifiable when it is no longer relevant.

Professionalism must characterize all dealings of the healthcare personnel who provide their services online. They must abide by their codes of ethics in dealing with their online clients or patients, they must put their clients interests first, and protect their confidentiality. These providers must make clear any constraints they may have in providing online consultation.

These online providers must be cautious in their professional associations, and that they practice Responsible Partnering in the associations they keep. They must be sure that any of these partners would not unduly influence or manipulate the responses or data they provide to their clients.

Finally, Accountability means that the user is made aware that if the service or consultation provided through the web site is not to their satisfaction, they have recourse to appeal to higher management of the site. They should know that they will be heard and satisfaction provided where required.

This, in a very abridged form, is the eHealth Code of Ethics. What makes it unique is its source, the Coalition, and that in a training program slide show, "HIPAA Training +: Beyond Compliance to Culture Change", Lois Ambash, PhD, and John Mack, M.A., maintain that the eight guiding principles of the Code coincide with those of the Health Insurance Portability and Accountability Act [(13)]. Those principles are "Openness, Individual Participation and Rights, Security, Accountability, and Limits on use, collection, and disclosure of information".

However, if one were to consider that the membership and affiliations of the Internet Healthcare Coalition include academic institutions, medical libraries, "medical specialty and special interest societies", "patient advocacy and support groups", and medical industry product manufacturers, and that one of their guiding ideas is that "the imposition of external controls on Internet sources of healthcare information" would be ineffective at best, or stifle the Internet marketplace for healthcare business, perhaps the parallels between the eHealth code of Ethics and these HIPAA principles may not seem so coincident. In any case, the eHealth Code of Ethics was meant to address the concerns about healthcare on the Internet and the implications of HIPAA regulation [(14)].

The point of presenting this code of ethics here is that there is much uncertainty about the real impact of the HIPAA regulatory and accountability provisions on the IT industry. Our areas of involvement are more specialized in the areas of access, security, data integrity and privacy. And under Responsible Partnering, they mean our employers and us as the partners. This code can be applied to any of us just

as it would to any online doctor or nurse. The ongoing speculation about the liability repercussions arising from HIPAA and that uncertainty will remain for some time I would suspect. Having a copy of this eHealth Code of Ethics posted on your wall and following it scrupulously is no guarantee that you will not feel the heat in the aftermath of any breach of faith, law, or rules. But if you understand this code of ethics, and the others mentioned here, you should have a sound basis to understand and navigate the provisions and repercussions of such legalistic megaliths as HIPAA.

Conclusion:

So in the end, whatever code of ethics you work under everyday is that which you hold onto yourself, one that you brought to the job with you, and/or it is that which is promulgated through your work environment. An organizational code should thread through your work culture, as Mitch Betts, Winn Schwartau and Malcolm Lloyd have shown in their writings cited here. And it will influence for better or for worse, depending on the culture that the organization fosters in your workaday world. Any organization that can imbue their workplace with the principles of an honest and forthright code of ethics is going to have profound influence on the ethical decision-making of their employees. If that code is perceived as window dressing, as something done to simply meet regulatory or customer expectations, it can have an opposite and detrimental affect.

Again, in their own ways all of these writers point out that an ethical behavior in an organization must start with a policy and that policy must be made part of the everyday way of doing things in the organization.

Malcolm Lloyd uses a mechanism of the "four P's": they are "Policy, Promote, Police, and Prosecute", to describe effective organizational policy implementation and maintenance. (Lloyd, page 16) Begin with the written policy, of which we have seen some very good examples; promote the code of ethics through all the usual media to reach all employees, and training. This would include visible ethics training sessions for upper management as well as for the lower echelons. Policing means steps such as establishing an organizational ethics ombudsman and providing policy and business decision review to validate the ethical practices followed. The point is to show there is a sincere effort made to monitor the ethical behavior of upper management as well the lower levels of the organizational pyramid. Finally, is policing followed through with prosecution of those at all levels who may violate the code of ethics? Prosecution may be forfeiture of pay, firing, or even civil or criminal charges.

There is no guarantee that every employee will now feel the obligation to stick to the ethical rules of the organization. The code of ethics is a facet of the organization and if an employee feels the need and obligation to the organization to stay within those rules, he will take on those rules as his own at least to some

degree. If an employee does not feel the requirement to follow the rules and breaks them, the weight of the organization and of the individuals within it will be aligned against him. In civil and criminal proceedings the existence of the code of ethics and the evident fact that the ethics code is a real part of the organizational culture does help protect the organization, at least to some degree, from liability for the actions of an individual. Next, we should remember the fiduciary responsibilities we discussed before. One of the responsibilities is that simple ignorance is no excuse, so the organization does have some responsibility to police itself. There is some expectation that the organization should be able to detect and deter the aberrant actions of individuals and, thus, stop the behavior before it comes to violations of civil or criminal law. This implies an aggressive ethics code promotion and policing within the organization at all levels. Passivity will impart some of the responsibility for the individual to the organization.

No matter if the organization itself is responsible to provide and promote a code of ethics for all to abide by, each individual starts out with at least some rudimentary personal guidelines. And at the end of the day, choice is still up to the individual.

References

1. Merriam Webster Collegiate Dictionary, Merriam-Webster Online URL: http://www.m-w.com/dictionary (7 Oct. 2002)

2. Fox, Pimm "South Carolina Law Puts IT in Disturbing Role", ComputerWorld, August 20, 2001 URL: http://www.computerworld.com/managementtopics/management/story/0,10801,63118,00.html (7 Oct. 2002)

3. Krebs, Brian, "Cybersecurity Draft Plan Soft on Business, Observers Say" Thursday, September 19, 2002; 12:00 AM washingtonpost.com Staff Writer URL: http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A35812-2002Sep18&notFound=true (7 Oct. 2002)

4. Strassman, Paul A. "Practice ethical IT" ComputerWorld APRIL 03, 2000 URL: http://www.computerworld.com/news/2000/story/0,11280,44328,00.html (7 Oct. 2002)

5. Betts, Mitch "Dirty rotten scoundrels?" May 22, 1995 ComputerWorld URL:http://www.computerworld.com/news/1995/story/0,11280,15336,00.html (7 Oct. 2002)

6. Schwartau **,** Winn "Cyber ethics in the workplace*"* Network World, January 1, 2002 URL: http://www.nwfusion.com/columnists/2002/0121schwartau.html (8 Oct. 2002)

7. Lloyd, Malcolm "Running Head: RM900 Comprehensive: Fiduciary" RM900 – THE COMPREHENSIVE, A paper from Doctoral candidate Malcolm Lloyd Capella University – Fall 1999 (M. Lloyd's paper is available on request)

8. Schwartau, Winn "Needed: An Electronic Bill of Rights" Network World*,* July 2, 2001 URL: http://www.nwfusion.com/columnists/2001/0702schwartau.html (8 Oct. 2002)

9. Computer Ethics Institute "The Ten Commandments of Computer Ethics" 16 April 2001. The Brookings Institution, Washington, D.C. URL: http://www.cpsr.org/program/ethics/cei.html, (4 Oct. 2002)

10. Association for Computing Machinery "Bylaw 15. ACM Code of Ethics and Professional Conduct" Last Update: 06/01/98 by Haritini Kanthou Bylaws of the Association of Computing Machinery URL: http://www.acm.org/constitution/bylaw15.html (3 Oct. 2002)

11. Crigger, Bette-Jane, "Foundations of the eHealth Code of Ethics" November, 2001, The Hastings Center, Internet Healthcare Coalition URL: http://www.ihealthcoalition.org/ethics/code-foundations.html (8 Oct. 2002)

12. Internet Healthcare Coalition, "eHealth Code of Ethics" 18 May, 2000 URL: http://www.ihealthcoalition.org/ethics/code0524.pdf (8 Oct. 2002)

13. Ambash, Lois, PHD; Mack, John, MA, M. Phil "HIPAA Training +: Beyond Compliance to Culture Change", The Internet Healthcare Coalition URL: http://www.ehcca.com/presentations/HIPAA4/3_06.ppt. (8 Oct 2002)

14. Internet Healthcare Coalition, "Statement of Purpose", 2000 URL: http://www.ihealthcoalition.org/about/who.html (8 Oct. 2002)

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event