Component 4/Unit 2/Part 4

Audio Transcript

Welcome to component 4 which is titled Introduction to Information and Computer Science. This is unit 2 entitled Internet and the World Wide Web.

You might wonder why this material needs to be covered. It seems to be ubiquitous - the internet and the world wide web are known by everybody, it seems. And yet many folks don’t understand its implications, its origins, how to use it, its advantages and disadvantages. Those are the topics that we’ll covered in this unit – I hope you enjoy the course.

Our unit objectives include gaining the abilities to define the internet and the world wide web, understand how to connect to the internet and various options available to you through your ISPs including IP addressing, DNS, domain names and then the fees associated with internet access.

Searching the internet, filtering results and evaluating credibility of results, internet security and privacy concerns, ethical considerations through the use of the internet, and finally, online health care applications and associated security and privacy issues and this will include a small discussion about HIPPA, which is the Health Insurance and Portability Act.

The open nature of the internet introduces ethical considerations that we did not have to consider before the internet existed. For example, in some apartments or small neighborhoods, folks will gather to share an internet connection with neighbors, perhaps one home purchases an internet connection then installs a wireless access point to be shared by the other neighbors. So this raises the question, “Should neighbors have the ability to pull together, lease an internet connection from an ISP and pay for sharing one connection?” Currently this practice is not legal.

And what about downloading software from the internet? Should licensed key generater sites be allowed to operate at all? Should they be shut down? Should people be allowed to download pirated software from the internet? Pirating software is a copyright infringement and selling unauthorized copies of commercial software are usually done at a very low price. All of this is currently illegal and yet in the first case of the key generator sites, they do exist.

What about downloading music and movies from the internet? Should people be able to download music without paying for it? And should people be able to download movies without paying for them?

What about copyright infringement? What are the ethical concerns for buying or using college research papers found on line? For example, you might visit a website and see a complete paper on a topic that you need to write about. Should you be able to purchase that paper and turn it in? If you purchase a paper of that sort, is it copyright infringement? Is it plagiarism? And the big question is, “Did you learn anything?”

And what about internet databases? Should companies be able to gather information about your surfing habits and then sell this information to marketing companies? What if they sold the information without providing your personal information? Would that be OK? Should the government have your surfing, banking and credit card history at its disposal?

We all know that everything on the internet is not true, don’t we? With this in mind, should companies or people be able to post false information in blogs, consumer ratings and so on? And along those lines, what is the law? And who defines it? What problems do you see in implementing this type of law?

Today it seems like everyone’s online. And often many of us feel like we’re on information overload. We know it seems so much about so many people and companies. When debit cards emerged, many people refused to use them because of privacy and security concerns. Indeed, today, many people will not use a debit card. But today many people are comfortable with online banking and they are comfortable conducting business over the internet.

Social networking sites make it easy for us to share personal information about ourselves in online communities, even though this does subject us to some type of privacy invasion. For example, if you post your birth date, your mother’s maiden name and your address and so on this might enable an attacker to impersonate you because now they know personal information. They might know where you’ve gone to school, what your dog’s name is, and the information that’s shown here on the screen - they might contact the credit card company and say that you’ve lost your credit card and ask it to be resent and make that happen

Well, with all of the social networking and the opportunity that exists for us to be violated, we have ask the question, “What is privacy?” Today most privacy law revolves around privacy between a person and the government. According to Wikipedia, the law of privacy regulates the type of information that which may be collected and how this information may be used and stored. In other words, privacy relates to people.

Which leads us to confidentiality. We should note that confidentiality is not the same as privacy. According to Wikipedia, confidentiality is commonly applied to conversations between doctors and patients. Legal protections prevent physicians from revealing certain discussions with patients even under oath in court. The rule only applies to secrets shared between physician and patient during the course of providing medical care. So in other words, confidentiality relates to data.

With consumer concerns about privacy and confidentiality and no really prevailing federal law to protect people, the HIPPA - the Health Insurance Portability and Accountability Act was introduced and enacted in 1996 by the US federal government. HIPPA requires that healthcare providers, insurance companies and employers abide by privacy and security standards. If you look at the slide notes for this slide, I’ve posted the Wikipedia link to HIPPA so you can you learn more about it. You might take a moment now and pause the presentation and look at that website.

Two important pieces of HIPPA relate to privacy and security. First let’s turn our attention to the privacy rule. HIPPA requires that those covered by the act provide patients a Notice of Privacy Practices when care is first provided. The privacy rule covers paper and electronic private health information.

The security rule goes further than the privacy rule, in that it covers administrative, physical and technical data safeguards that must be enacted to secure electronic health record data. In other words how is the data transported across the internet and so on.

Many of the concerns related to medical privacy are due to the fact that there are a number of electronic health records available for use by your doctor and by you. If you use a personal health record system, this means that you can maintain it. Notice that this is different than an electronic health system, or an HER system. PHRs are maintained by you and are not covered by HIPPA rules because you manage your health record, not the company that’s providing you with the ability to have the health record.

And some links here from GoogleHealth, Microsoft Health Vault and WebMD’s health manager will give you an idea as to the types of PHRs that are available . Typically these are free and allow you to enter all of your medical information in them and share them with your doctor if you choose so.

Electronic health records, or EHRs, are used by healthcare providers. EHRs are maintained by healthcare providers. They’re covered by HIPPA rules and so the privacy security rules that we mentioned apply here. EHRs utilize centralized database systems to integrate patient intake, medical care, pharmacy, billing, images and so on into one large database system. Departments or entities may not be in the same physical location so this means that patient data most likely has to travel over the internet to get from one destination to another.

People can view their own health record, taking ownership of its contents, ensuring accuracy and so on. And so in this case you would have access to your entire record that existed at your hospital or within your region, personally.

And finally, this leads us to some electronic health record security questions and answers. And so the question, “How is my data sent over the internet?” is answered in that it is sent in an encrypted secure manner over the internet. Is my data safe? Much depends on an organization’s physical records and network security practices. But we should really keep in mind that no data with ever be 100 percent secure against theft or misuse. Who can view my health records? Only those who need to know or view the contents of your health record should be able to view it.

And finally, you must authorize all other access.

<end>