**Chapter 10**

**Data Security**

*Laurie A. Rinehart-Thompson, JD, RHIA, CHP, FAHIMA*

**Real-World Case 10.1**

In 2014, the Department of Health and Human Services reported on its website a $4.8 million HIPAA settlement with New York and Presbyterian Hospital (NYP) and Columbia University following the 2010 breach of thousands of patients’ e-PHI. A Columbia University physician, who was an attending physician at NYP, tried to deactivate a computer server that he owned on the network that contained NYP patient e-PHI. The e-PHI became accessible to the public on Internet search engines because technical safeguards were lacking. A patient’s loved one found e-PHI about the patient on the Internet and filed a complaint.

In addition to the impermissible disclosure, both entities were noncompliant in other ways: (1) no attempts had been made to assure the server was secure; (2) a thorough risk analysis had never been completed that identified all systems able to access the e-PHI of NYP patients and therefore no plan to address potential threats and hazards existed; (3) no appropriate policies and procedures existed regarding authorizing access to its databases; and (4) they did not follow their own policies on information access management (HHS 2014).

This costly mistake, both monetarily and from a reputation standpoint, highlights the negative outcomes that can happen when both technical and administrative safeguards are not followed. It also emphasizes the importance of inventorying all systems and devices that can access an organization’s e-PHI to address threats and an organization’s vulnerabilities. This is not an easy task given the number of personal and mobile devices that access e-PHI, but it is critical.

US Department of Health and Human Services (HHS). 2014 (May 7). Data Breach Results in $4.8 million HIPAA Settlements. http://www.hhs.gov/news/press/2014pres/05/20140507b.html.

# Real-World Case Discussion Questions

1. A risk analysis should include an inventory of all systems and devices that can access an organization’s ePHI (in this case, the breach occurred via a physician’s personal computer server). How can an organization account for all systems and devices on which PHI may be accessed or otherwise present? **All users of any device to access phi need to be registered with the organization all user should have to account for each of their devices and make sure they are protected.**

2. What should the risk analysis include? **Possible security threats and weakness in security threats how to deal with threats and likelihood of them. Also the impact of such threats weakness and strengths of security protection**

3. Should the physician have been the one to deactivate the server? Why or why not**? I think the hospital technical security dept should be the only ones to deactivate the server they are more skilled in threat and security breaches and their impact**

**Real-World Case 10.2**

Riverside Health System in Virginia announced in 2014 that the e-PHI of nearly 1,000 patients was breached by a nurse who accessed Social Security numbers and EHRs. The violation was discovered during a random organizational audit. Riverside described its compliance program as robust with ongoing monitoring (McCann 2014). This case raises numerous issues; for example, the fact that humans present one of the greatest threats to data security. When this human threat is internal to the organization, it is heightened by the ability to access information in the course of doing business. The article did not describe what type of access was given to employees; however, a nurse role is likely to result in broad access. The inappropriate access had occurred over a four-year period, which raises the issue of monitoring adequacy. Nonetheless, monitoring was taking place. The nurse was terminated after the breach was discovered. When the perpetrator of the breach was identified, all electronic access for that person should have been terminated immediately as well.

McCann, E. 2014 (January 2). 4-Year Long HIPAA Breach Uncovered. HealthITNews. http://www.healthcareitnews.com/news/four-year-long-hipaa-data-breach-discovered.

# Real-World Case Discussion Questions

1. What red flags does this case raise? **Training for staff, too much access more then needed to do job poor oversight in monitoring due to duration of breach.**

**2.** How would you have avoided this breach**? More monitoring at least monthly documted yearly training of staff and only allow access to information needed to do job.**

3. Alternatively, given limited human resources that most organizations have to conduct audits, is it realistic to conclude that monitoring truly was robust and this breach still occurred, undetected? **I don’t think so 4 years is much too long to go undected maybe more software or programs could have prevented it.**

# Application Exercises

*Instructions:* Answer the following questions.

1. Search the Internet for news about security breaches in healthcare and other industries in the last three years. Make a summary of each case. Identify the principal threats in each of these cases and what could have been done to minimize the threats**. Most of the cases seem to have the result of human error either intention or deliberate. More training and monitoring of employees would have helped also limiting access to only needed info to complete their job**

## 2. Search the Internet for as many sites as you can that are concerned with health information privacy and security. Make a list of the sites and provide a two- or three-sentence description of each. What are the biggest security concerns expressed on each site? Share and compare the sites during a classroom session with your classmates. [Healthcare Data Solutions | symantec.com](https://1751992.r.bat.bing.com/?ld=d3rnL1wurp90QwVwhhopX4SzVUCUzKIr-wo5HtkZSH-jhIQ7QnL5xrYZuwbUSY3YL9ItfxlIyYrg-9lD-mVZS9CZVf5wUMdkQMCU5cvtKpVKaWM67luYbOijBw-Y-kM3nzWMzKMer-Zv6eOuBJgmYZnr18k4wWzZI_V0ivBug7PlEQvVb6&u=https%3a%2f%2fwww.symantec.com%2fcampaigns%2fhealthcare-solutions%3f%26om_sem_cid%3dbiz_sem_187476831216112%7cpcrid%7c73323690531119%7cpmt%7cb%7cplc%7c%7bplacement%7d%7cpdv%7cc)

Ad · [*www.symantec.com*](https://1751992.r.bat.bing.com/?ld=d3rnL1wurp90QwVwhhopX4SzVUCUzKIr-wo5HtkZSH-jhIQ7QnL5xrYZuwbUSY3YL9ItfxlIyYrg-9lD-mVZS9CZVf5wUMdkQMCU5cvtKpVKaWM67luYbOijBw-Y-kM3nzWMzKMer-Zv6eOuBJgmYZnr18k4wWzZI_V0ivBug7PlEQvVb6&u=https%3a%2f%2fwww.symantec.com%2fcampaigns%2fhealthcare-solutions%3f%26om_sem_cid%3dbiz_sem_187476831216112%7cpcrid%7c73323690531119%7cpmt%7cb%7cplc%7c%7bplacement%7d%7cpdv%7cc) · Site secured by Norton

## [Learn Mo](https://1751992.r.bat.bing.com/?ld=d3rnL1wurp90QwVwhhopX4SzVUCUzKIr-wo5HtkZSH-jhIQ7QnL5xrYZuwbUSY3YL9ItfxlIyYrg-9lD-mVZS9CZVf5wUMdkQMCU5cvtKpVKaWM67luYbOijBw-Y-kM3nzWMzKMer-Zv6eOuBJgmYZnr18k4wWzZI_V0ivBug7PlEQvVb6&u=https%3a%2f%2fwww.symantec.com%2fcampaigns%2fhealthcare-solutions%3f%26om_sem_cid%3dbiz_sem_187476831216112%7cpcrid%7c73323690531119%7cpmt%7cb%7cplc%7c%7bplacement%7d%7cpdv%7cc)

***[www.wikihow.com](https://1751992.r.bat.bing.com/?ld=d3rnL1wurp90QwVwhhopX4SzVUCUzKIr-wo5HtkZSH-jhIQ7QnL5xrYZuwbUSY3YL9ItfxlIyYrg-9lD-mVZS9CZVf5wUMdkQMCU5cvtKpVKaWM67luYbOijBw-Y-kM3nzWMzKMer-Zv6eOuBJgmYZnr18k4wWzZI_V0ivBug7PlEQvVb6&u=https%3a%2f%2fwww.symantec.com%2fcampaigns%2fhealthcare-solutions%3f%26om_sem_cid%3dbiz_sem_187476831216112%7cpcrid%7c73323690531119%7cpmt%7cb%7cplc%7c%7bplacement%7d%7cpdv%7cc)****[/](https://1751992.r.bat.bing.com/?ld=d3rnL1wurp90QwVwhhopX4SzVUCUzKIr-wo5HtkZSH-jhIQ7QnL5xrYZuwbUSY3YL9ItfxlIyYrg-9lD-mVZS9CZVf5wUMdkQMCU5cvtKpVKaWM67luYbOijBw-Y-kM3nzWMzKMer-Zv6eOuBJgmYZnr18k4wWzZI_V0ivBug7PlEQvVb6&u=https%3a%2f%2fwww.symantec.com%2fcampaigns%2fhealthcare-solutions%3f%26om_sem_cid%3dbiz_sem_187476831216112%7cpcrid%7c73323690531119%7cpmt%7cb%7cplc%7c%7bplacement%7d%7cpdv%7cc)****[Protect](https://1751992.r.bat.bing.com/?ld=d3rnL1wurp90QwVwhhopX4SzVUCUzKIr-wo5HtkZSH-jhIQ7QnL5xrYZuwbUSY3YL9ItfxlIyYrg-9lD-mVZS9CZVf5wUMdkQMCU5cvtKpVKaWM67luYbOijBw-Y-kM3nzWMzKMer-Zv6eOuBJgmYZnr18k4wWzZI_V0ivBug7PlEQvVb6&u=https%3a%2f%2fwww.symantec.com%2fcampaigns%2fhealthcare-solutions%3f%26om_sem_cid%3dbiz_sem_187476831216112%7cpcrid%7c73323690531119%7cpmt%7cb%7cplc%7c%7bplacement%7d%7cpdv%7cc)****[-](https://1751992.r.bat.bing.com/?ld=d3rnL1wurp90QwVwhhopX4SzVUCUzKIr-wo5HtkZSH-jhIQ7QnL5xrYZuwbUSY3YL9ItfxlIyYrg-9lD-mVZS9CZVf5wUMdkQMCU5cvtKpVKaWM67luYbOijBw-Y-kM3nzWMzKMer-Zv6eOuBJgmYZnr18k4wWzZI_V0ivBug7PlEQvVb6&u=https%3a%2f%2fwww.symantec.com%2fcampaigns%2fhealthcare-solutions%3f%26om_sem_cid%3dbiz_sem_187476831216112%7cpcrid%7c73323690531119%7cpmt%7cb%7cplc%7c%7bplacement%7d%7cpdv%7cc)****[Health](https://1751992.r.bat.bing.com/?ld=d3rnL1wurp90QwVwhhopX4SzVUCUzKIr-wo5HtkZSH-jhIQ7QnL5xrYZuwbUSY3YL9ItfxlIyYrg-9lD-mVZS9CZVf5wUMdkQMCU5cvtKpVKaWM67luYbOijBw-Y-kM3nzWMzKMer-Zv6eOuBJgmYZnr18k4wWzZI_V0ivBug7PlEQvVb6&u=https%3a%2f%2fwww.symantec.com%2fcampaigns%2fhealthcare-solutions%3f%26om_sem_cid%3dbiz_sem_187476831216112%7cpcrid%7c73323690531119%7cpmt%7cb%7cplc%7c%7bplacement%7d%7cpdv%7cc)****[-](https://1751992.r.bat.bing.com/?ld=d3rnL1wurp90QwVwhhopX4SzVUCUzKIr-wo5HtkZSH-jhIQ7QnL5xrYZuwbUSY3YL9ItfxlIyYrg-9lD-mVZS9CZVf5wUMdkQMCU5cvtKpVKaWM67luYbOijBw-Y-kM3nzWMzKMer-Zv6eOuBJgmYZnr18k4wWzZI_V0ivBug7PlEQvVb6&u=https%3a%2f%2fwww.symantec.com%2fcampaigns%2fhealthcare-solutions%3f%26om_sem_cid%3dbiz_sem_187476831216112%7cpcrid%7c73323690531119%7cpmt%7cb%7cplc%7c%7bplacement%7d%7cpdv%7cc)****[Information](https://1751992.r.bat.bing.com/?ld=d3rnL1wurp90QwVwhhopX4SzVUCUzKIr-wo5HtkZSH-jhIQ7QnL5xrYZuwbUSY3YL9ItfxlIyYrg-9lD-mVZS9CZVf5wUMdkQMCU5cvtKpVKaWM67luYbOijBw-Y-kM3nzWMzKMer-Zv6eOuBJgmYZnr18k4wWzZI_V0ivBug7PlEQvVb6&u=https%3a%2f%2fwww.symantec.com%2fcampaigns%2fhealthcare-solutions%3f%26om_sem_cid%3dbiz_sem_187476831216112%7cpcrid%7c73323690531119%7cpmt%7cb%7cplc%7c%7bplacement%7d%7cpdv%7cc)***

[Jul 29, 2015 · Edit Article](https://1751992.r.bat.bing.com/?ld=d3rnL1wurp90QwVwhhopX4SzVUCUzKIr-wo5HtkZSH-jhIQ7QnL5xrYZuwbUSY3YL9ItfxlIyYrg-9lD-mVZS9CZVf5wUMdkQMCU5cvtKpVKaWM67luYbOijBw-Y-kM3nzWMzKMer-Zv6eOuBJgmYZnr18k4wWzZI_V0ivBug7PlEQvVb6&u=https%3a%2f%2fwww.symantec.com%2fcampaigns%2fhealthcare-solutions%3f%26om_sem_cid%3dbiz_sem_187476831216112%7cpcrid%7c73323690531119%7cpmt%7cb%7cplc%7c%7bplacement%7d%7cpdv%7cc) **[How to Protect Health Information](https://1751992.r.bat.bing.com/?ld=d3rnL1wurp90QwVwhhopX4SzVUCUzKIr-wo5HtkZSH-jhIQ7QnL5xrYZuwbUSY3YL9ItfxlIyYrg-9lD-mVZS9CZVf5wUMdkQMCU5cvtKpVKaWM67luYbOijBw-Y-kM3nzWMzKMer-Zv6eOuBJgmYZnr18k4wWzZI_V0ivBug7PlEQvVb6&u=https%3a%2f%2fwww.symantec.com%2fcampaigns%2fhealthcare-solutions%3f%26om_sem_cid%3dbiz_sem_187476831216112%7cpcrid%7c73323690531119%7cpmt%7cb%7cplc%7c%7bplacement%7d%7cpdv%7cc)**[. Community Q&A.](https://1751992.r.bat.bing.com/?ld=d3rnL1wurp90QwVwhhopX4SzVUCUzKIr-wo5HtkZSH-jhIQ7QnL5xrYZuwbUSY3YL9ItfxlIyYrg-9lD-mVZS9CZVf5wUMdkQMCU5cvtKpVKaWM67luYbOijBw-Y-kM3nzWMzKMer-Zv6eOuBJgmYZnr18k4wWzZI_V0ivBug7PlEQvVb6&u=https%3a%2f%2fwww.symantec.com%2fcampaigns%2fhealthcare-solutions%3f%26om_sem_cid%3dbiz_sem_187476831216112%7cpcrid%7c73323690531119%7cpmt%7cb%7cplc%7c%7bplacement%7d%7cpdv%7cc) **[Health information](https://1751992.r.bat.bing.com/?ld=d3rnL1wurp90QwVwhhopX4SzVUCUzKIr-wo5HtkZSH-jhIQ7QnL5xrYZuwbUSY3YL9ItfxlIyYrg-9lD-mVZS9CZVf5wUMdkQMCU5cvtKpVKaWM67luYbOijBw-Y-kM3nzWMzKMer-Zv6eOuBJgmYZnr18k4wWzZI_V0ivBug7PlEQvVb6&u=https%3a%2f%2fwww.symantec.com%2fcampaigns%2fhealthcare-solutions%3f%26om_sem_cid%3dbiz_sem_187476831216112%7cpcrid%7c73323690531119%7cpmt%7cb%7cplc%7c%7bplacement%7d%7cpdv%7cc)** [is gathered as you seek preventative care or treatment for](https://1751992.r.bat.bing.com/?ld=d3rnL1wurp90QwVwhhopX4SzVUCUzKIr-wo5HtkZSH-jhIQ7QnL5xrYZuwbUSY3YL9ItfxlIyYrg-9lD-mVZS9CZVf5wUMdkQMCU5cvtKpVKaWM67luYbOijBw-Y-kM3nzWMzKMer-Zv6eOuBJgmYZnr18k4wWzZI_V0ivBug7PlEQvVb6&u=https%3a%2f%2fwww.symantec.com%2fcampaigns%2fhealthcare-solutions%3f%26om_sem_cid%3dbiz_sem_187476831216112%7cpcrid%7c73323690531119%7cpmt%7cb%7cplc%7c%7bplacement%7d%7cpdv%7cc)

[re About Trending Threats & Cyber Security Risks in](https://1751992.r.bat.bing.com/?ld=d3rnL1wurp90QwVwhhopX4SzVUCUzKIr-wo5HtkZSH-jhIQ7QnL5xrYZuwbUSY3YL9ItfxlIyYrg-9lD-mVZS9CZVf5wUMdkQMCU5cvtKpVKaWM67luYbOijBw-Y-kM3nzWMzKMer-Zv6eOuBJgmYZnr18k4wWzZI_V0ivBug7PlEQvVb6&u=https%3a%2f%2fwww.symantec.com%2fcampaigns%2fhealthcare-solutions%3f%26om_sem_cid%3dbiz_sem_187476831216112%7cpcrid%7c73323690531119%7cpmt%7cb%7cplc%7c%7bplacement%7d%7cpdv%7cc) **[Healthcar](https://1751992.r.bat.bing.com/?ld=d3rnL1wurp90QwVwhhopX4SzVUCUzKIr-wo5HtkZSH-jhIQ7QnL5xrYZuwbUSY3YL9ItfxlIyYrg-9lD-mVZS9CZVf5wUMdkQMCU5cvtKpVKaWM67luYbOijBw-Y-kM3nzWMzKMer-Zv6eOuBJgmYZnr18k4wWzZI_V0ivBug7PlEQvVb6&u=https%3a%2f%2fwww.symantec.com%2fcampaigns%2fhealthcare-solutions%3f%26om_sem_cid%3dbiz_sem_187476831216112%7cpcrid%7c73323690531119%7cpmt%7cb%7cplc%7c%7bplacement%7d%7cpdv%7cc)**

**** [**Protecting Personal Health Information in Research ...**](http://privacyruleandresearch.nih.gov/pr_02.asp)

*privacyruleandresearch.nih.gov/pr\_02.asp*

Apr 14, 2003 · Research on Decedents’ **Protected Health Information**; Other Uses and Disclosures of **Protected Health Information**; Minimum Necessary Restriction;

**** [**Protected Health Information - Health IT makes it possible ...**](https://www.healthit.gov/patients-families/what-you-can-do-protect-your-health-information)

***www.healthit.gov****› … ›* [***Protecting*** *Your Privacy & Security*](https://www.healthit.gov/patients-families/protecting-your-privacy-security)

Your medical records are **protected health information**. Find out the extra steps you can take to **protect** your **health information**.

3. View the security breaches affecting 500 or more individuals posted on the Office for Civil Rights website at <https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf>. Instruct the students to categorize the breaches by type and location of breached information. Are most large breaches intentional or negligent? What medium presents the greatest risk for a breach? Have the students select three cases and list ways (using HIPAA security rule requirements and news articles about the breaches) that these breaches might have been avoided**. Most breeches were theft related most occurred from laptop or desk top computer. So, I would say most breeches are caused by human error from their use of computers. MOST breeches are unintentional and caused by negligent These breeches could have been elimated by having proper protocols in place and training and more monitoring of computer data use and the need to protect it. More audit trails could help**

4. Inventory the security policies of a healthcare organization in your area. Use the following table to help organize your inventory. Share your inventory during a class session or in a class presentation with your classmates. Compare and contrast how these policies meet HIPAA security provisions.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Policy name and**  **date of policy**  THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATON.  PLEASE REVIEW IT CAREFULLY.  This Notice of Privacy Practices (Notice) will be followed by all Central Maine Healthcare Corporation (CMH) hospitals, service delivery sites, physician practices, long term care facilities, healthcare workers and staff.  CMH is committed to protecting the confidentiality of your medical information, and are required by law to do so.  This Notice describes how we may use your medical information and how we may disclose it to others.  The Notice also describes the rights you have concerning your own medical information.  Please review it carefully and let us know if you have questions.   We will ask you to sign an acknowledgement that you received this Notice.  We regard the safeguarding of your personal identifiable information as an important duty.  The elements of this notice and the consents &/or authorizations you sign are required by state and federal law for your protection.  We have in place safeguards to protect the privacy of your information.  Our staff is regularly trained on the obligation to protect the privacy of our patients.  We hold medical records in a secure area.  Only staff members that have a “need to know” are permitted access to your medical records or other information.  Our staff understands the legal and ethical obligation to protect your information.  A violation of this Notice of Privacy Practices will result in disciplinary action.  HOW WILL WE USE YOUR MEDICAL INFORMATION AND SHARE IT WITH OTHERS?  Treatment:  We may use your medical information to provide you with medical services and supplies.  We may also share your medical information with others who need to treat you.  This includes; doctors, physician assistants, nurses, medical and nursing students, technicians, therapists, emergency service and medical transportation providers, medical equipment providers, medical imaging technologists, and others involved in your care.  For example, we will allow your physician to have access to your medical record to assist in your treatment and for follow-up care.  We participate in a state-wide arrangement of healthcare organizations who have agreed to work with each other to make available electronic health information that may be relevant to your care.  This is called HealthInfoNet (“HIN”) and allows Maine hospitals, doctors and other health care providers to quickly share certain health information about their patients.  For example, if you are admitted to a hospital participating in HealthInfoNet on an emergency basis and cannot provide important information about your health condition, this arrangement will help those who need to treat you at the hospital to see your health information held by another participating provider.  When it is needed, ready access to your health information means better care for you.  You may choose to not make your protected health information available to this state-wide arrangement by completing an “opt-out” election form available online, or from your provider’s office. Upon request, CMHC will submit the opt-out form to HealthInfoNet for you, at 125 Presumscot Street, Box 8, Portland, ME  04103.  For further information you can visit their website at [www.hinfonet.org](http://www.hinfonet.org/) or give them a call at (207) 541-9250 or 1-866-592-4352.  We may contact you to remind you of an upcoming appointment, to inform you about possible treatment options, or to tell you about health-related services available to you.  We will use and share your medical records in an emergency to ensure you receive the necessary medical services.  If there is a substantial communication barrier and we try but cannot obtain your consent, and your doctor, using his or her professional judgment, concludes that you would consent to the use or disclosure of your medical record, the necessary information will be shared.  Patient Directory:  To help family members and visitors locate you while you are in the Hospital, the Hospital has a patient directory.  This directory includes your name, your general condition, where you are in the Hospital, and religion (if any) to be given to the clergy. This information is only given out to those who ask for you by name.  You have the option, at registration, to limit who has access to this information.  Family Members and Others Involved in Your Care:  We may share your medical information with a family member or friend who is involved in your medical care or to someone who helps pay for your care. For example when a patient is not present or without capacity, we may allow a third party to pick up prescriptions, supplies, or x-rays.  We also may share your medical information with disaster relief organizations to help locate a family member or friend in a disaster.  If you do not want us to share your medical information with family members or others, please let us know.  Decedent Information: Surviving family members or other persons involved in your care will have continued access to your personal medical information, unless you previously expressed preferences to the contrary. Otherwise you will be protected by these privacy rules for a period of 50 years following the date of death.  Payment:  We may use and share your medical information to get paid for the medical services and supplies we provide to you.  For example, your health plan or health insurance company may ask to see parts of your medical record (chart) before they will pay us for your treatment.  Health Care Operations:  We may use and share your medical information if it is necessary to improve the quality of care we provide to patients or to run the facility.  We may use your medical information to look for ways to improve your care. For example, we may look at your medical record (chart) to evaluate whether staff, your doctors, or other health care professionals did a good job.  Research:  We may use or share your medical information for research projects, such as studying how well a type of treatment worked.  These research projects must go through a special process that protects the confidentiality (privacy) of your medical information. We are prohibited from using or disclosing your genetic information for underwriting purposes.  Required by Law:  Federal, state, or local laws sometimes require us to share patients’ medical information. For instance, we are required to report child abuse or neglect and must provide certain information to law enforcement officials in domestic violence cases.  We also are required to give information to the State Workers’ Compensation Program for work-related injuries.  Public Health:  We may report certain medical information for public health purposes.  We may need to report patient problems with medications or medical products to the Food and Drug Administration (FDA) or notify patients of recalls of products they are using. In some circumstances we may need to notify schools of immunization records and once received by the school they are protected by another set of privacy guidelines.  Public Safety:  We may share medical information for public safety purposes in limited circumstances.  We may share medical information to law enforcement officials in response to a search warrant or a grand jury subpoena.  We may share medical information to assist law enforcement officials in identifying or locating a person.  To prosecute a crime of violence, to report deaths that may have resulted from criminal conduct, and to report criminal conduct at the facility.  We may share your medical information to law enforcement officials and others to prevent a serious threat to health or safety.  Health Oversight Activities:  We may share medical information with a government agency that oversees the Facility or its staff, such as the State Department of Health & Human Services, the federal agencies that oversee Medicare, the Board of Medical Examiners or the Board of Nursing.  These agencies need medical information to watch how well we follow state and federal laws.  Coroners, Medical Examiners and Funeral Directors:  We may share medical information concerning patients who have died to coroners, medical examiners and funeral directors.  We may share medical information to groups that handle organ, eye or tissue donation or transplantation.  Military, Veterans, National Security and Other Government Purposes:  If you are a member of the armed forces, we may release your medical information as required by military command authorities or to the Department of Veterans Affairs.  We may share medical information to federal officials for intelligence and national security purposes, or for presidential Protective Services.  Judicial Proceedings:  We may share medical information if a court orders us to or if we receive a search warrant.  Information with Additional Protection:  Certain types of medical information have additional protection under state or federal law.  For instance, medical information about HIV/AIDS, mental health, and alcohol and drug abuse treatment has more protection in Maine.  We are required in many circumstances to get your permission before sharing this information.   Other Uses and Disclosures:  If we wish to use or share your medical information for a reason that is not discussed in this Notice, we will seek your permission.  If you give your permission, you may change your mind at any time, unless we have already relied on your permission to use or share the information.  If you want to change your mind about sharing your medical information, please notify the Privacy Office in writing.  WHAT ARE YOUR RIGHTS?  Right to Request Your Medical Information:  You have the right to look at your own medical information and to get a copy.  (The law requires us to keep the original record.)  This includes your medical record, your billing record, and other medical records we use to make decisions about your care. To request a copy of your medical information, write to the Medical Records Department.  We will respond to your request as soon as possible, but no later than 30 days from the date of your request.   When you request a copy of your information, we will tell you then how much the copy will cost. You can look at your record at no cost. You also have the right to your medical records in an electronic format that is suitable to you at cost.  However, you do not have the right to psychotherapy notes or information gathered in reasonable anticipation of a civil, criminal, or administrative proceeding.  Your right of access may be limited if providing this information could endanger the health or safety of yourself or others.  Right to Request Changes to your Medical Information:  If you look at your medical information and believe that some of the information is wrong or incomplete, you may submit a request to have it fixed.  To request a change, write to the Medical Records Department.  We will respond as soon as possible, but no later than 60 days from the date of your request.  If we deny your request, you have the right to submit a written statement of reasonable length disagreeing with the denial.  We then have the right to send a rebuttal statement.  Right to Get a List of Certain Disclosures of Your Medical Information:  You have the right to request a list of many of the disclosures we make of your medical information.  This list does not include information used for treatment, payment, health care operations or any information released with your consent.  If you would like to get a copy of the list, write to the Medical Records Department.  We will respond as soon as possible, but no later than 60 days from the date of request.  We will provide the first list to you free, but we may charge you for any additional lists you request during the same year.  We will tell you in advance what this list will cost.  Right to Request Restrictions on How We Will Use or Share Your Medical Information for Treatment, Payment, or Health Care Operations:  You have the right to request us not to share your medical information for your treatment, payment for care, or to operate the facility.  We are required to agree to such requests if the disclosure of information is to a health plan regarding payment or health care operations and the protected health information relates to an item or service that has been paid for out of pocket in full to the provider AND the disclosure is not required by law. We are not required to agree to your requests that do not match these criteria, but if we do agree, we will comply with that agreement.  If you want to make a request that we not share your information, you must make this request in writing to the Medical Records Department and describe your request in detail.  Right to Request Private Communications:  You have the right to ask us to communicate with you in a way that you feel is more private.  For example, you can ask us not to call your home, but to contact you only by mail.  To do this, you must make this request in writing of the office at which you receive your care.  Right to a Paper Copy:  If you have received this notice electronically, you have the right to a paper copy at any time. You may download a paper copy of the notice from our Web site, at [www.cmmc.org](http://www.cmmc.org/) or you may obtain a paper copy of the notice at any CMH Office.  **CHANGES TO THIS NOTICE**  From time to time, we may change our practices concerning how we use or share patient medical information, or how we will protect patient rights concerning their information.  We reserve the right to change this Notice and to make the provisions in our new Notice effective for all medical information we maintain.  If we change these practices, we will publish a revised Notice of Privacy Practices.  You can get a copy of our current notice of Privacy Practices at any time by stopping in any of CMH locations or from the website.  **WHICH HEALTH CARE PROVIDERS ARE COVERED BY THIS NOTICE?**  This Notice of Privacy Practices applies to our personnel, volunteers, students, and trainees.   The Notice also applies to other health care providers that come to our facility to care for patients, such as physicians, physician assistants, therapists, and other health care providers who are not employed by us, unless these other health care providers give you their own Notice that describes how they will protect your medical information.   We may share your medical information with these providers for treatment purposes, payment and health care operations.  This arrangement is solely for sharing information and not for any other purpose.  **DO YOU HAVE CONCERNS OR COMPLAINTS?**  Please tell us about any problems or concerns you have with your privacy rights or how we use or share your medical information.  If you have a concern, please contact the Privacy Contact at your facility as listed at the end of this Notice.  If for some reason we cannot resolve your concern, you may also file a complaint with the federal government at Region 1, Office for Civil Rights, U.S. DHHS, JFK Federal Building – Room 1875, Boston, MA 02203; phone (617) 565-1340 or TDD (617) 565-1343.  We will not penalize you or retaliate against you in any way for filing a complaint with the federal government.  **DO YOU HAVE QUESTIONS?**  We are required by law to give you this Notice and to follow the terms of the Notice that is currently in effect.  It is also our responsibility to notify any affected individuals if there has been a breach of your unsecured personal health information. If you have any questions about this Notice, or have further questions about how we may use and share your medical information, please contact the Privacy Officer for Central Maine Healthcare at the number listed, or your local practice or department                                                                                                                                      CMH HOSPITAL LOCATIONS AND SERVICE DELIVERY SITES, ALONG WITH PRIVACY CONTACT AND PHONE NUMBER Office 207-795-0111 or Privacy Hotline 207-795-2906  **CMH HOSPITAL PRIVACY CONTACT AND PHONE NUMBERS**   |  |  | | --- | --- | | Bridgton Hospital 10 Hospital Drive Bridgton, Maine 04009 Privacy Contact (207) 647-6000 | Central Maine Medical Center 300 Main Street Lewiston, Maine  04240 Privacy Officer (207) 795-2281 | | Rumford Hospital 420 Franklin Street Rumford, ME  04276 Privacy Contact (207) 369-1000 | Central Maine Healthcare Confidential Compliance & Privacy Hotline  (207)795-2906  Or email at: Compliance\_and\_Privacy\_Hotline@cmhc.org |      * [Advance Directives](https://www.cmmc.org/inpatient-advance-directives) * [Arbor House](https://www.cmmc.org/inpatient-arbor-house) * [Contacting Patients](https://www.cmmc.org/inpatient-contacting-patients) * [Discharge](https://www.cmmc.org/inpatient-discharge) * [Food Services](https://www.cmmc.org/inpatient-food-services) * [Gift Shop](http://giftshop.cmmc.org) * [Human Ethics Committee](https://www.cmmc.org/inpatient-human-ethics-committee) * [Interpreters](https://www.cmmc.org/inpatient-interpreters) * [Newspapers](https://www.cmmc.org/inpatient-newspapers) * [Notary Public](https://www.cmmc.org/inpatient-notary-public) * [Pastoral Care](https://www.cmmc.org/inpatient-pastoral-care) * [Pet Therapy](https://www.cmmc.org/inpatient-pet-therapy) * [Patient Representatives](https://www.cmmc.org/inpatient-representatives) * [Privacy Statement](https://www.cmmc.org/inpatient-privacy-statement) * [Smoking](https://www.cmmc.org/inpatient-smoking) * [Special Services](https://www.cmmc.org/inpatient-special-services) * [Student Nurses](https://www.cmmc.org/inpatient-student-nurses) * [Telephone](https://www.cmmc.org/inpatient-telephone) * [Television](https://www.cmmc.org/inpatient-television) * [Visiting Hours](https://www.cmmc.org/inpatient-visiting-hours) | **Summary of policy** | **Complies with which HIPAA sections**  It complies |
|  |  |  |
|  |  |  |

**Review Quiz**

*Instructions:* For each item, complete the statement correctly or choose the most appropriate answer.

1. Data security includes protecting data availability, privacy, and \_\_\_\_\_\_\_\_.

a. Suitability

**b. Integrity**

c. Flexibility

d. Quality

2. Within the context of data security, protecting data privacy means defending or safeguarding \_\_\_\_\_\_\_\_\_.

**a. Access to information**

b. Data availability

c. Health record quality

d. System implementation

3. The greatest threat category to electronic health information is which of the following?

a. Natural disasters

b. Power surges

c. Hardware malfunctions

**d. Humans**

4. The first and most fundamental strategy for minimizing security threats is which of the following?

**a. Establish access controls**

b. Implement an employee security awareness program

c. Establish a secure organization

d. Conduct a risk analysis

5. Administrative safeguards include policies and procedures that address which of the following regarding computer resources?

**a. Management**

b. Maintenance

c. Modification

d. Manipulation

6. The individual responsible for ensuring that everyone follows the organization’s data security policies and procedures is which of the following?

a. Chief executive officer

b. Chief information officer

c. Chief privacy officer

**d. Chief security officer**

7. An employee accesses PHI on a computer system that does not relate to her job functions. What security mechanism should have been implemented to minimize this security breach?

**a. Access controls**

b. Audit controls

c. Contingency controls

d. Security incident controls

8. A visitor to the hospital looks at the screen of the admitting clerk’s computer workstation when she leaves her desk to copy some admitting documents. What security mechanism would best have minimized this security breach?

a. Access controls

b. Audit controls

**c. Automatic logoff controls**

d. Device and media controls

9. A laboratory employee forgot his user ID badge at home and uses another lab employee’s badge to access the computer system. What controls should have been in place to minimize this security breach?

a. Access controls

b. Security incident procedures

c. Security management process

**d. Workforce security awareness training**

10. A dietary department donated its old microcomputer to a school. Some old patient data were still on the microcomputer. What controls would have minimized this security breach?

a. Access controls

**b. Device and media controls**

c. Facility access controls

d. Workstation controls

11. HIPAA requires that policies and procedures be maintained for a minimum of \_\_\_\_\_\_\_.

a. Seven years

b. Six years from date of creation

**c. Six years from date of creation or date when last in effect, whichever is later**

d. Seven years from date when last in effect

12. A visitor walks through the computer department and picks up a CD from an employee’s desk. What security controls should have been implemented to prevent this security breach?

a. Device and media controls

**b. Facility access controls**

c. Workstation use controls

d. Workstation security controls

13. Threats to data security are most likely to come from which of the following?

**a. Employees**

b. Natural disasters

c. Compromised firewalls

d. Hackers outside an organization

14. These are automatic checks that help preserve data confidentiality and integrity.

a. Access controls

**b. Audit controls**

c. Application controls

d. Incident controls

15. An employee in the physical therapy department arrives early every morning to snoop through the EHR for potential information about neighbors and friends. What security mechanism should have been implemented that could minimize this security breach?

a. Audit controls

**b. Facility access controls**

**c. Facility access controls**

d. Workstation security

16. An employee observes an outside individual putting some computer disks in her purse. The employee does not report this security breach. What security measures should have been in place to minimize this threat?

a. Access controls

b. Audit controls

c. Authentication controls

**d. Security incident procedures**

17. Locks on computer room doors illustrate a type of \_\_\_\_\_\_\_\_\_.

**a. Access control**

b. Workstation control

c. Physical control

d. Security breach

18. An admission coordinator consistently enters the wrong patient gender while entering data in the MPI. What security measures should be in place to minimize this security breach?

a. Access controls

b. Audit trail

**c. Edit checks**

d. Password controls

19. Which of the following statements is true regarding HIPAA security?

a. All institutions must implement the same security measures.

**b. HIPAA allows flexibility in the way an institution implements the security standards**.

c. All institutions must implement all HIPAA implementation specifications.

d. A security risk assessment must be performed every year.

20. For HIPAA implementation specifications that are addressable, the covered entity \_\_\_\_\_\_\_\_\_.

a. Implements the specification

b. May choose not to implement the specification if it is too costly to execute

**c. Must conduct a risk assessment to determine if the specification is appropriate to its environment**

d. Does not have to implement the specification if it is a small hospital

21. A user recently opened a file that they thought would help them with their job but it copied files to unsecure ares of the computer. What thpe of malware was activated?

a. Rootkit

b. Computer virus

c. Computer work

**d. Trojan horse**

22. Training that educates employees on the confidential nature of PHI is known as which of the following?

**a. Awareness**

b. Risk

c. Incident

d. Safeguard

23. “Something you have” is demonstrated by:

a. CAPTCHA

b. Retinal scan

c. Password

**d. Token**

24. Policies are which type of safeguards?

a. Technical

b. Application

**c. Administrative**

d. Network

25. A hospital is looking to use something to act as a buffer between two networks. What should be recommended?

a. Application control

b. Cryptography

**c. Firewall**

d. Digital certificate