

Name: _____

USC ID: _____

INF 529 Midterm Exam

Spring 2016

Instructions:

Show all work. No electronic devices are allowed. This exam is open book, open notes. You have **120 minutes** to complete the exam.

Please prepare your answers on separate sheets of paper. You may write your answers on the sheet of paper with the question (front and back). If you need more space, please attach a separate sheet of paper to the page with the particular question. **Do NOT extend your answer on the back of the sheet for a different question, and do NOT use the same extra sheet of paper to answer more than one question.** The exam will be split apart for grading by different people, and if part of your answer for one question appears on a page given to a different grade because the sheet contains parts of the answer to more than one question, then you will NOT receive credit for that part of the answer not seen by the grader. In particular, **each numbered questions must appear on separate pieces of paper so that the exam can be split for grading.**

Be sure to include your **name** and **USC ID** number **on each page.**

There are **100 points** in all and **3 questions.**

	Q1	Q2	Q3		Total Score
Score					

Name: _____

USC ID: _____

Privacy and Security for Healthcare -

As consumers we demand instant access to healthcare related data on an increasing basis. From portability requirements for access to data so that test results from one physician are available to others, to our ability to review the data personally, and eventually our ability to manage data from personal devices such as the Fitbit, monitoring our heartrate, activities, and much more. Included in health data are medical records containing diagnoses and prescribed medications, as well as medical histories including information about family members, various "risky" activities like smoking, drinking, and unprotected sex. The results of medical labs such a blood tests and x-rays will be included. For some individuals, this data may also include genetic characteristics, such as what can be obtained from the service 23 and me which sequences an individuals genome and provide information about ancestry and susceptibility to various Medical conditions. This information may also contain payment information and identifying information like name, address, phone number, and social security numbers.

The data above may need to be protected in terms of confidentiality, integrity, and availability. One example of a recent breach to availability of data is the ransomware incident at Hollywood Presbyterian Hospital where data was encrypted by malicious software and a \$3 Million ransom was demanded to restore the data. The Hospital eventually paid approximately \$17,000, but the impact to their operations was more significant.

All three of the questions that follow pertain to systems being developed to collect, analyze, share, and utilize this collection of heath related information.

- 1) What are the consequences of compromise of the health data described above? In describing the consequences, explain what might happen as a result of a breach of confidentiality, integrity, or availability for specific pieces of data described above. Mention the consequences to the individuals whose data is compromised, as well as consequences to the holder of that information. What might other entities be able to with such data if they gain access to the data? (Answer on the rest of this page and on the back of this page). (30 points)

Name: _____

USC ID: _____

- 2) For each kind of healthcare related information describe in the introduction to this exam (1st half of page 2), list who should have access to the data and the kind of access (e.g. ability to read the data, create the data, and modify the data). Describe any special constraints that should apply to this access. Finally, suggest where in the system (e.g. on a server managed by X, on a patients computer, on a patients mobile device, etc) would be the best place or places to store this data to best protect it? (40 points)

Name: _____

USC ID: _____

- 3) Discuss some approaches that can be taken to protect the data against privacy, integrity, and availability threats. These measures can be technical or legal and may be taken by the holder of the data, by the subject of the data (the patient), or by others. Among other things, these approaches may involve the way the data is stored or transmitted, the structure of the systems that will process or store the data (including technical defenses applied on those systems) or the steps taken when one seeks to access the data. In answering this question, consider the kinds of attacks (social engineering, malicious code/viruses) etc that we discussed in class. (30 points)