AIMS OF THE APPLIED SESSION

1) Reflect and discuss the importance of human-centred design in dealing with uncertain, messy and complex information ecosystems
2) Reflect and discuss the importance of human-centred design in IS security design

STRUCTURE OF THIS WEEK'S APPLIED SESSION

- Section A: Group Creation Reminder (10 min)
- Section B: Mini Case 1 (The Trouble with "Users" is They're Only Human) (30 min)
- Section C: Mini Case 2 (Security and Controls at New Mexico Health Systems) (30 min)
- **Break (10 min)**
- Section D: In-applied class Quiz 1 (15 min)
- Section E: Figma Setup (45 min)
- Section F: Assignment 1 Q&A (30 min)

YOUR TASKS

BEFORE YOUR APPLIED SESSION

- Attend/listen to seminar 3
- Read the mini-cases
- Prepare requirement for Figma Education Plan e.g. copy of your class schedule, proof of enrollment / employment or a copy of your transcript
- Watch four videos about Figma:
  - Figma For Beginners: Explore ideas (1/4)
  - Figma For Beginners: Create designs (2/4)
  - Figma For Beginners: Build prototypes (3/4)
  - Figma For Beginners: Prepare for Handoff (4/4)

IN YOUR APPLIED SESSION

You will work with your fellow students and tutor through the Week 3 Applied activities.

Section A: Group Creation Reminder	Your tutor will remind you to form groups of 5 for the Group Assignment. The groups must be finalised by Week 3.

Section B: Mini Case 1 (The Trouble with "Users" is They're Only Human)	**The Trouble with "Users" is They're Only Human** Great advances were made in electronics and computing throughout the second half of the 20th century. The problem was, the designers of many systems often overlooked the human limitations of the people who had to interact with them. Early computers were extremely hard to understand. The first ones — created in the 1940s — required specialists to operate them in closed environments. By the 1980s, things had changed; A large portion of smaller computers were being used by people without specialist knowledge. Problems were bound to arise, and did. The early Unix system Ed (for "Editor"), for example, did not prompt users to save their changes, causing many users to erase their work when turning off their computers. Highly visible prompts to save our work were yet to come. From no save prompts, to the "Do you want to save changes" dialog box, to auto-save: The save functionality in documents has been iterated over the years to improve the experience for the people working with these tools. Don Norman also studied the control rooms of potentially hazardous industrial centers and aviation safety. Following the Three Mile Island nuclear accident in 1979, he was involved in analysing the causes and potential solutions. A partial meltdown of a power-station reactor had released dangerous radioactive material into the environment. The problem centered around, not the highly competent staff members, but the design of the control room itself. From design mistakes such as this, we learned crucial lessons. It was clear that designers had to accommodate the human needs of their systems' usership. There could be no room for ambiguity or misleading controls, for instance. Designers would instead have to anticipate human users extensively through how each system looked, worked and responded to them, which aligns with circular economy principles to maximise resource efficiency and sustainability. So, rather than focus on the aesthetics of the interface and the design itself, designers needed to understand and tailor experiences for the people at the controls, accounting for their various states of mind while interacting with and reacting to changes in the system. To avoid disasters, the dehumanising idea of "users" had to vanish so designers could put people first in design. It was time for human- or, better still, people-centered design. Source: Interaction Design Foundation - IxDF. (2021, June 14). What is Human-Centered Design (HCD)?. Interaction Design Foundation - IxDF. https://www.interaction-design.org/literature/topics/human-centered-design Source: How do bad, and in some cases – life-threatening – designs, occur? https://amber-mcgregor.co.uk/essay/designing_badly.html Answer and discuss the following questions: B1) How critical is it to include humans or end-users in systems design? Why? B2) What are the negative impacts if humans do not become the centre of the systems design? Give an example. B2) Why could bad design happen? How to avoid bad systems design? Be prepared to share your findings.
Section C: Mini Case 2 (Security and Controls at New Mexico Health Systems)	**Security and Controls at New Mexico Health Systems** Jim Gutierrez was hired three months ago by New Mexico Health Systems (NMHS) to oversee all software development projects. Though Jim lacked prior experience in health-care services, he'd been hired due to excellent performance in software development projects for a variety of firms in various industries. His skills in designing and deploying

complex mobile applications were especially valuable for several projects in progress at NMHS, including a reimplementation of the billing and insurance reimbursement system and an upgrade to the patient portal that enables patients to view their medical records and to interact with their primary care providers via a secure messaging system.

From his first week on the job, Jim was concerned about security and controls within NMHS's existing systems and those under development. Jim gained little traction with senior management when he raised those concerns, but they did agree to let him hire an outside consultant. Consequently, he'd hired Alice Watts, a security consultant with extensive health-care-related experience, to complete a thorough analysis of existing systems and to make recommendations for securing the systems under development. Alice's analysis had taken almost a month to complete. Jim had received some disturbing preliminary findings as the work progressed, but he hadn't yet seen the complete report.

At a meeting that included upper management, Alice presented her report. She began, "Though I'll cover several security-related issues in my presentation, I want to start by saying that there is far more good news than bad about the security of your infrastructure and your existing systems. You have an excellent network administrator. She's hardened your network and web systems within it against malicious attacks. Bright spots include extensive encryption of data at rest and in transit, robust user authentication and authorisation methods, and a well-implemented hierarchy of access controls for your hardware, operating systems, databases, and applications."

Alice continued, "Though your infrastructure security methods do much to protect your systems from external attacks, I did find that internal threats, which plague all systems, are a hit-or-miss proposition. For example, your system for sharing recorded notes by physicians does not encrypt data between your internal networks and devices. Also, there's no requirement for device-level encryption or approval by a supervisor or the health-care provider. Because your physicians use a wide variety of devices, you need additional controls to ensure the integrity of patient medical records—especially for follow-up orders for lab tests, prescriptions, and downstream care coordination."

Rajesh Kumar, the financial officer, interrupted, "We're planning a pilot for an expensive text-to-speech system that will eliminate the need for transcription. We were hoping to avoid spending any more time and resources on the current system."

Alice replied, "While I understand the sentiment, you're opening yourself to medical errors and lawsuits in the interim. One litigation-related malpractice suit could easily cost you far more than technology updates for the current system."

Jim added, "I've investigated this issue further since Alice alerted me a couple of weeks ago. I think that we can make the needed changes in a matter of weeks for about $20,000."

Diana Lourdes (the chief medical officer) replied while glancing at Rajesh, "I think that's a prudent investment."

Alice continued, "There are a few other easy-to-resolve issues with existing systems. But I'd like to skip over them to what I think are much more important topics. My biggest security-related concerns are with your two systems under development—especially the patient portal. Both systems open internal and external systems to outside access. The billing application has some weaknesses despite controls implemented within the Web services interface. But the patient portal is your biggest risk because it breaks new ground by enabling mobile browser-based access from ordinary users with untrusted devices. Your current design, development, and deployment methods aren't up to the task of fully securing such a system. The risk of malicious attacks or accidental data release through the patient portal is very high. You can't fully mitigate that risk with infrastructure-related security and controls bolted on to the system after it's been developed. You have to design the security and controls into every part of the software and the underlying support system."

	Rajesh interrupted with a conservative concern, "Is this project in danger? Do we need to start over?" Alice replied, "I wouldn't go that far, but some immediate changes are needed. I'll provide an executive summary of my recommendations here. Then, I'll invite your lead developers and operations managers to discuss these points in more detail. As part of that discussion, I'll provide you with comparative data about similar systems in health care and other industries, as well as specific case studies about security risks." Source: John W. Satzinger, Robert B. Jackson, and Stephen D. Burd. Systems Analysis and Design in a Changing World | 7th Edition Answer and discuss the following questions: C1) What problems did Alice identify and report to the management at NMHS? C2) *"…there's no requirement for **device-level encryption or approval by a supervisor or the health-care provider**. Because your physicians use a wide variety of devices, you need additional controls to ensure the integrity of patient medical records—especially for follow-up orders for lab tests, prescriptions, and downstream care coordination…."* If you are the systems analyst that will analyse the design for such a requirement (device-level encryption or approval by a supervisor or the health-care provider), how would you analyse and design a solution so that it can consider the end-user (physicians)? C3) *"…You can't fully mitigate that risk with infrastructure-related security and controls bolted on to the system after it's been developed…."* Why do you think Alice made this statement?
Section D: **In-applied class Quiz 1**	
Section E: **Figma Setup**	This activity aims to prepare you and your teams to use Figma in the following weeks. Make sure you have created a New Account, create a Team, and Invite your team member along with your Tutor to your Team. 1. If you have already formed your group, please sit together. Ensure you have watched all four Figma tutorial videos assigned prior to this session. 2. Create a New Account in Figma using your Monash Account. 3. Create a **New Team** in Figma and name it based on the group name registered in the Google Sheet/Form. 4. Invite your **team members** and your **tutor** to join your Figma team. 5. Go to https://www.figma.com/education/apply to apply for the Figma Education Plan. 6. Show your tutor that you have completed all the steps to confirm that you are ready for next week's Figma activity.
Section F: **Assignment 1 Q&A**	