

IMPROPER HIPAA DISCLOSURE CAN:

- Cause pain and suffering among individuals whose privacy is harmed.
- Undermine public's trust in institutions that collect and hold the data.
- Cost organizations' their creditability and future access to data.
- Lead to significant financial repercussions on organizations and staff.

CHALLENGES TO ENSURING DATA SECURITY:

- The healthcare system is more computer-dependent and integrated.
- More people have access to protected health information.
- There are many opportunities for data to be accidentally or intentionally disclosed, lost, or stolen.
- Stealing personal health information is financially rewarding.
- Data security depends as much on staff awareness as security technology.
- Smaller organizations must effectively raise staff awareness with limited funding.
- Security awareness materials lose effectiveness quickly after the initial viewing.

EFFECTIVE DATA SECURITY REQUIRES STAFF TO:

- Be aware of policies and sanctions.
- Understand the background of HIPAA.
- Sign acknowledgements that they understand the policies and sanctions.
- Know their security responsibilities.
- Know whom to turn to in case a security risk occurs and to have that contact information ready.
- Receive and review security reminders.

JEN'S GOALS FOR ITS SECURITY AWARENESS VIDEO PROCESS:

- Low cost: As JEN is a small organization, the process needed to be relatively low-cost both in development and implementation.
- Easily adapted: To make the most of JEN's investment, as well as to address how quickly technology and security rules can change, the process needed to be easily adapted for other uses, e.g., other staff training, client training, and marketing materials.
- In-house: To keep costs low and to increase the production speed, the entire process needed to be accomplished in-house.

MINIMAL EQUIPMENT IS NEEDED:

- Big pads of paper and pencils for drawing.
- Software:
 - Video-making software: Used to make the actual videos. Cost ~\$300.
 - Graphics editing programs: Used to make vector art for the videos and to adjust the images. These were not absolutely necessary, but they did improve our visual aspects. Cost ranges from \$50 - 80 per month.
- Video equipment:
 - HD Camcorder, cost ~ \$400; Recording Microphone for all the voice-overs, cost ~ \$50; Photo/Video Tripod, cost ~ \$12.

STEPS JEN TOOK IN DESIGNING, IMPLEMENTING, AND REFINING THE VIDEO PROCESS:

1. GATHERING

1. Create a team

- The team needs: subject matter expertise; ability/willingness to learn how to make videos; available time.

2. Collect the security content

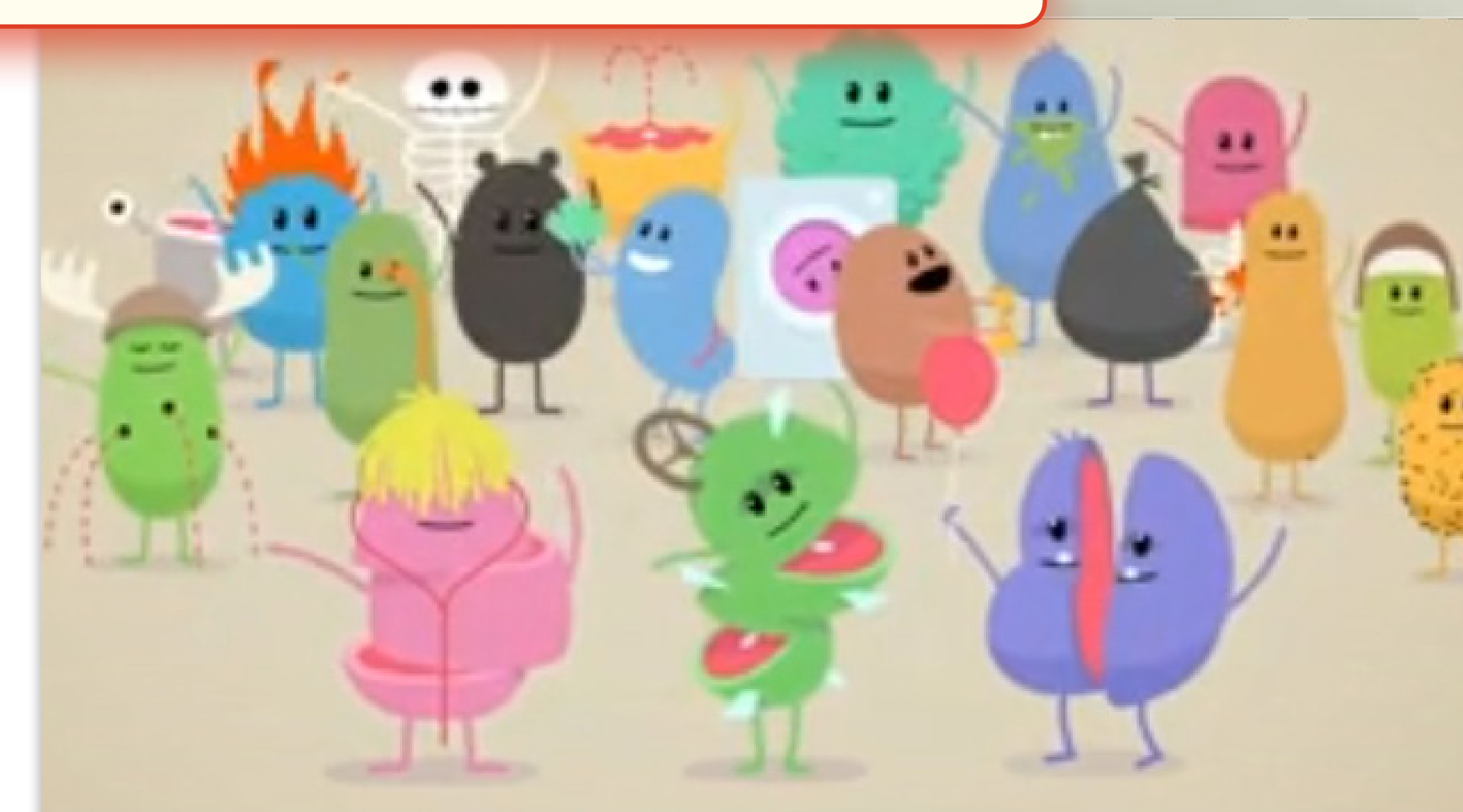
- We chose to start with our security policies.

3. Research visual examples to find a feasible style

- We searched the web and chose to start with the whiteboard example as that most closely fit our abilities.



"Obama and the Debt Ceiling: An Explainer," Peadar Kirby at Marketplace Money explains the debt ceiling.



"Dumb Ways to Die" from Melbourne Metro Trains. Part of a campaign aimed at preventing train-related deaths in Victoria, Australia.

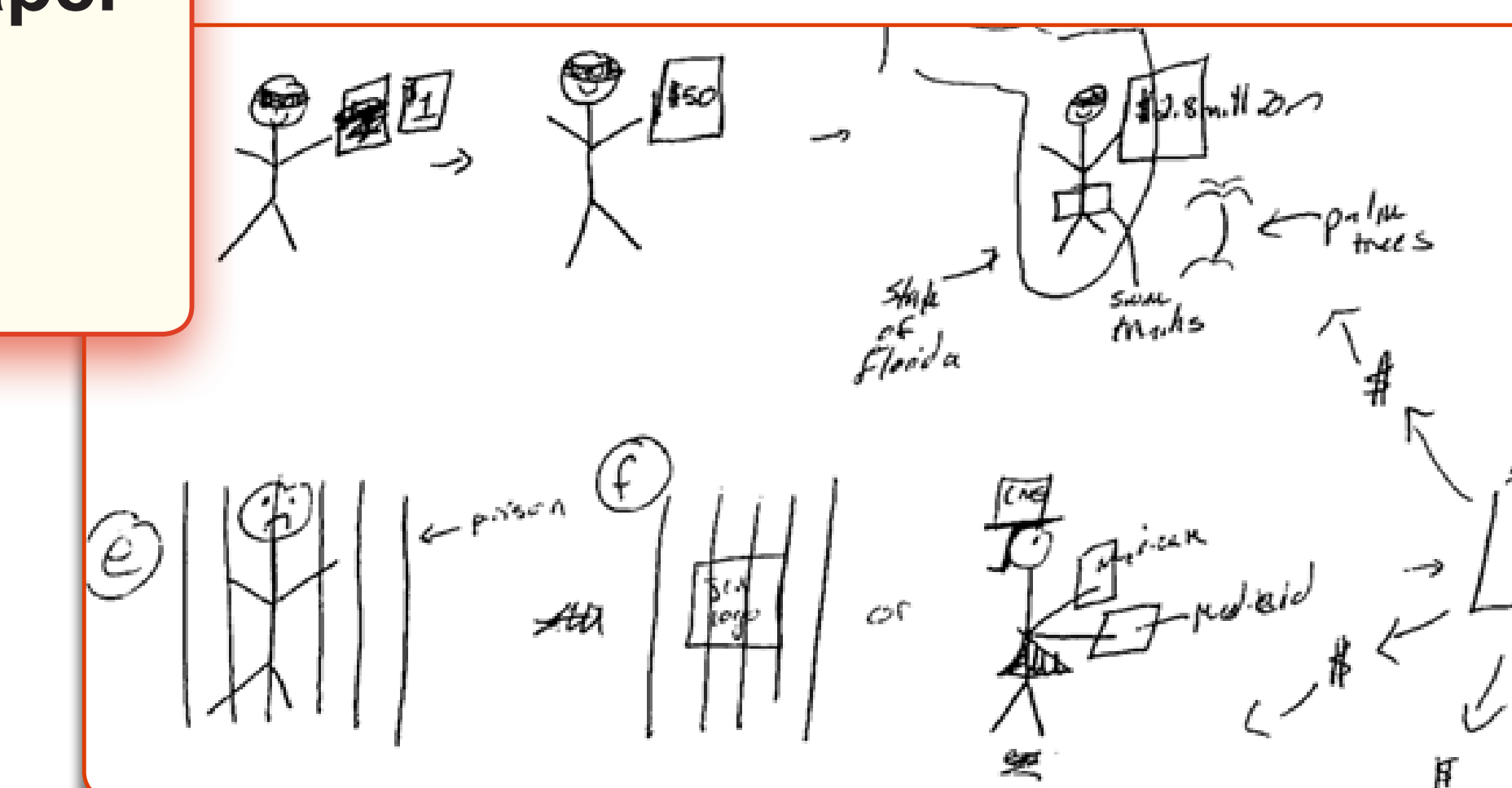


"How schools kill creativity." Animated by RSA Animate from a TED Talk given by Sir Ken Robinson.

2. DRAFTING

4. Map out the concept on paper

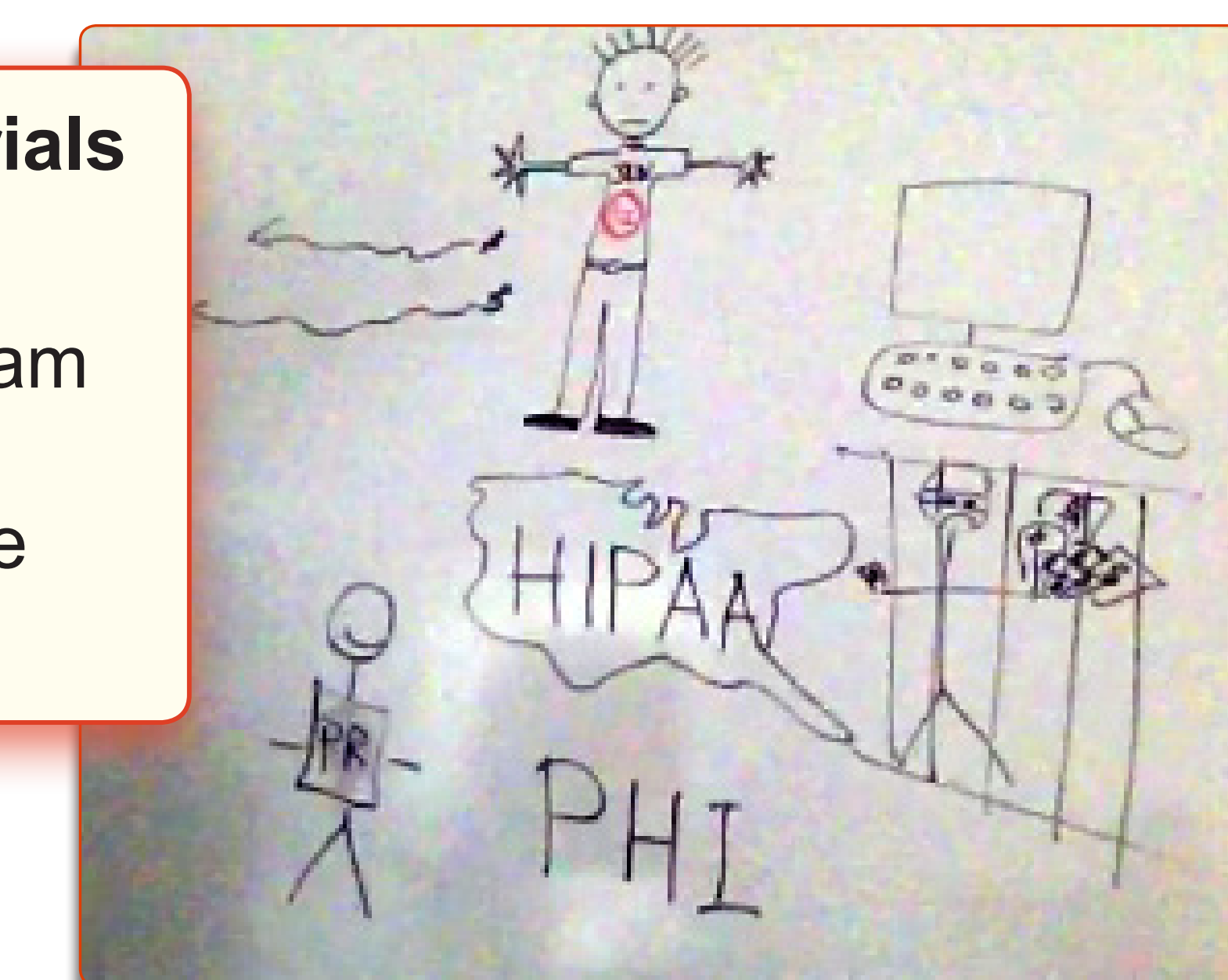
- We wrote out a script with a voiceover and stick figures.



Snapshot of the hand-drawn figures in the initial script.

5. Create an initial video with materials at hand to test out the concept

- We used a basic camera to film a team member drawing on a whiteboard with a coat blocking the light from the window.



Screenshot from initial recording of the first security video.

3. REFINING

6. Assess the video

- While the first video had charm, it clocked in at 21 minutes -- far too long to hold a staffperson's attention.
- We felt that the hand-drawn concept worked, but we moved from drawing on a whiteboard to paper.

7. Obtain additional needed equipment/software

- We invested under \$1000 in new equipment and software as we already had some of the software.

8. Reshoot the video

- We broke the script into smaller pieces to create a series of 3-5 minute videos that covered all the security policies.
- We edited the script down to the essential points.
- We also refined the drawings.



Screenshot from first completed security video.

4. REFLECTING

9. Develop lessons learned

- The upfront investment of time is high, but the process becomes faster and easier with each video.
- In terms of equipment and software, our total investment was fairly small. We considered it worthwhile since we were able to make videos for many different purposes.
- Low tech and inexpensive appearing videos can work in your favor since people are used to slick videos.
- While humor helps capture interest, it can be tricky; what is humorous to one person can be tiresome or offensive to another.
- The videos need to be short, ideally less than three minutes long. Be ruthless in your editing.
- Minimize the jargon.
- Keep switching up the video styles in order to maintain staff interest. We expanded beyond hand-drawn figures in our later videos.
- Add as much RAM as possible; otherwise your video files will crash all the time.