

E5 - Privacy Challenge Questions

1. Project manager asks, "why do we have to jump through one more bureaucratic hoop?"

- Access and Privacy is the Law
- Needed for approvals / decision-makers and stakeholders are risk-avoidant
- Due diligence

2. IT Manager says, "No need to worry about privacy, we have all the latest security measures in place."

- That's great! Now we need to document what you've done!
- Security does not equal privacy.
- Privacy is more than safeguards or confidentiality (Just 1 of FIPS)

3. Project Leader asks, "What can we do to get around all of these barriers in the Act?"

- That's not what's expected of you.
- We should look at the proposed design and see what's causing the problem
- Ultimately, you could go get legislative approval or amendments to authorize whatever it is you want to do, but it means going public.

4. Project Leader says, "Thanks for letting us know about the PIA – let us know when you're done."

- It's your project, your PIA, your responsibility to protect PI
- PIA is just a tool, you have to implement the recommendations
- The process can't be completed without your involvement and support.

5. There's no documentation. The program is based on a meeting decision back in 1973.

- You called me just in the nick of time!
- You'll need to assign someone to document the process.
- We may find there is a gap in terms of authority, so the PIA should point that out for resolution.

6. At initial PIA meeting you are told, "The system goes live next week"

- It will not be possible to complete the PIA in a week.
- If you launch, you should be aware that you will be taking risks. What risks, I don't know.
- Better start anyway.

7. In sign-off phase, the system owner says to you, the reviewer, "Will you sign the PIA?"

- No, not as a reviewer
- It's their project. They should have project owner sign (accept and implement recommendations)
- It's a decision-making tool. I'm not the decision-maker.

8. We just got a new supercomputer! We now have the capacity to collect and store more data!"

- Collection must be tied to legally authorized activity (public sector)
- Must assess risk and sensitivity of storing a lot of data in one place.
- Just because you can, doesn't mean you should.

9. My Director says that under FIPPA/PHIPA we don't have to do a PIA.

- Technically, he's right. FIPPA and PHIPA don't mention PIA's.
- Directors can decide not to do them, but they need to realize they may be putting their Minister's job (and their own) at risk. Minister's are accountable under FIPPA.
- PIA's are good business practice. End up with better quality projects.

10. You just finished drafting the PIA and the project scope changes.

- Is it significant?
- What's the risk?
- What's the impact?