We should always disaggregate data by sex.

In chaotic crisis situations, we can’t always be sure that the data we collect is reliable.

We should avoid using digital tools where women’s access to such technology is limited.

If we follow all these rules about data management, we’ll never get anything done.
If we follow all these rules about data management, we’ll put too much of a burden on communities.

Informed consent is about explaining why we’re collecting information and how we will use it.

The best place to interview teenage girls about sexual and reproductive health is in the privacy of their homes.

All participants in focus groups should agree to keep the discussions confidential.
We need to get a parent or guardian's consent before collecting data from children.

All personally identifying data such as names, addresses, phone numbers, and dates of birth should be treated as high risk, with specific safeguards put in place for their management.

Data protection laws don’t apply to humanitarian agencies working in other countries.

All humanitarian settings are high-risk contexts for data management.
We can reuse data, including images, that are already in the public domain.

Responsible data management is only relevant to staff who directly collect data in the field.

We can protect data better if we store it digitally.

We should always use mobile phones to collect data, as it’s more efficient.
Biometrics are a good way of verifying who people are and reducing fraud.

Using drones offers really exciting potential to get images from otherwise inaccessible areas.

We should always go back to communities and tell them what we did with the data we collected.

We should always encrypt files containing personal data.
We should always make distribution lists public, for reasons of transparency and accountability.

Digital data should always be encrypted or password-protected.

Physical copies of documents should be locked away.

As long as files are deleted, it’s OK to throw away old flash drives in the office bin.
We should never take identifiable photos of individuals in conflict zones.

In order to get better public support, humanitarians should use Twitter to post ‘live’ images of their day-to-day work.

If the national authorities ask us for programme data, we’re legally required to hand it over.

Using mobile phones to film is a great way to share information with colleagues about a situation.
Once we’ve collected information, it belongs to our organization and we can do whatever we want with it.

We shouldn’t tell people they can withdraw consent for us to use their data when in reality we have no way of doing what they ask.

We have a responsibility to do something with data once we’ve collected it.

It’s best to ask interviewees more questions the first time, so you don’t have to go back and ask more.
Being responsible means we can’t openly share data – we have to protect it.

Privacy is more important than transparency.

When it’s impossible to find female interpreters for minority languages, we need to be pragmatic and use men, or risk women’s voices not being heard.

To have credible global analysis, we should ask the same questions in the same way, wherever we are in the world.
To make data anonymous, we should remove all names.

Storing data on a local hard drive is safer than storing it in the Cloud.

Storing all the data we collect is very expensive and a huge strain on our systems.

We should make a plan for data deletion at the very start of a collection process.