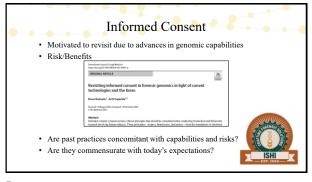
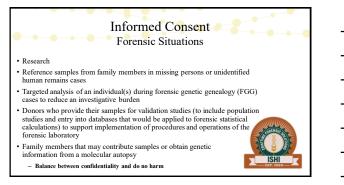


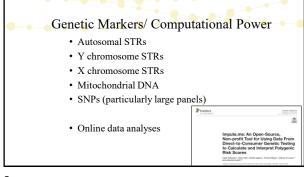
	Informed Cor	nsent
• Respect, Ber	neficence, Justice	
 Information, 	Comprehension, Volu	intary Participation
• Do no harm,	treat fairly and equall	ly, autonomy, no coercion
And the second s	Principles and Guidelines for the Protection of Human is of Research	RANGENCE CONTRACTOR INCOMENDATION INCOMENDATIONI INCOMENDATION
	CLARATION OF TAIPEI arch on Health Databases, Big Data and Biobanks	VUINERABILITY AND PRESONAL INTEGRITY Report of the biometrics Biodetic Convention of UNISCO BIAC











General Privacy Concepts					
Concept	Description				
Fit-for-purpose	Describe legitimate purposes and gather informed consent for collecting genomic and other personal data				
Data minimization	Collect only data necessary for the specified purpose				
Storage	Retain personal data and samples only as long as necessary for the specified purpose				
Transparency	Describe lawful and/or ethical basis for processing personal or genomic data in a fair, clear and understandable manner				
Confidentiality	Provide privacy and security of personal data and samples				
Accuracy	Ensure that personal data collected are correct, exact, up to date				



	General Security Measures					
to Mitigate Risk						
Measure	Description or risk	Mitigation examples				
Administrative controls	Data breach	Overall Information security program including training				
		Policies and procedures to prevent, detect, contain and correct data violations				
		Business/operation or data continuity plans and incident response plans				
	Accountability	Designated database steward or risk officer				
		Periodic external privacy impact studies				
	Unauthorized access	Internal and external authorization processes				
		Defined data retention policies for all files and stages of workflow				
		Response plan for risk assessed or unperceived issues				
Physical controls	Data access and availability	Designed database and storage mechanisms to limit proliferation of raw or processed dat				
		Inventory and logs on all systems that access and share data				
		System, data and user level controls for system monitoring, encryption, tokenization, etc				
Technical controls	Unauthorized access	Authorization and authentication mechanisms such as multifactor sign in				
		Registration of users				
		System access logs				
		Security of data when transmitted and during storage				
		User initiated data deletion				

